Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Appendix C

CMSR Low Impact Level Data

FINAL
Version 1.0
August 31, 2010

Document Number: CMS-CIO-STD-SEC01-1.0

(This Page Intentionally Blank)

Access Control (AC) – *Technical*

AC-1 – Access Control Policy and Procedures (Low)

Control

The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:
a. A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

Guidance

This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the access control family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the access control policy.

Applicability: All	**Reference(s):** FISCAM: AC-4, AS-1, SM-1, SM-3; HIPAA: 164.308(a)(3)(ii)(A), 164.308(a)(4)(ii)(C); IRS-1075: 5.6.3.2#1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AC-1.1

Assessment Objective

Determine if:
the organization develops and formally documents access control policy;

the organization access control policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented access control policy to elements within the organization having associated access control roles and responsibilities;

the organization develops and formally documents access control procedures;

the organization access control procedures facilitate implementation of the access control policy and associated access controls;

the organization disseminates formal documented access control procedures to elements within the organization having associated access control roles and responsibilities;

the organization reviews/updates the access control policy and procedures within every three hundred sixty-five (365) days.

Assessment Methods And Objects

Examine: Access control policy and procedures; other relevant documents or records.

AC-2 – Account Management (Low)

Control

The organization manages information system accounts, including:
a. Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary);
b. Establishing conditions for group membership;
c. Identifying authorized users of the information system and specifying access privileges;
d. Requiring appropriate approvals for requests to establish accounts;

e. Establishing, activating, modifying, disabling, and removing accounts;
f. Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts;
g. Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes;
h. Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users;
i. Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions; and
j. Reviewing accounts using the frequency specified in Implementation Standard 1.

Implementation Standard(s)

1. Review information system accounts within every three hundred sixty-five (365) days and require annual certification.
2. Remove or disable default user accounts. Rename active default accounts.
3. Implement centralized control of user access administrator functions.
4. Regulate the access provided to contractors and define security requirements for contractors.

Guidance

The identification of authorized users of the information system and the specification of access privileges is consistent with the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by organizational officials responsible for approving such accounts and privileged access.

Applicability: All	**Reference(s):** FISCAM: AC-2, AC-3, AC-4, AS-2, AS-4, BP-3, SD-2, SM-4; HIPAA: 164.308(a)(3)(ii)(B), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B); IRS-1075: 5.3#3, 5.6.3.2#2.1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AC-2.1

Assessment Objective

Determine if:
the organization manages information system accounts, including;
- identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary);
- establishing conditions for group membership;
- identifying authorized users of the information system and specifying access privileges;
- requiring appropriate approvals for requests to establish accounts;
- establishing, activating, modifying, disabling, and removing accounts;
- specifically authorizing and monitoring the use of guest/anonymous and temporary accounts;
- notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes;
- deactivating: (a) temporary accounts that are no longer required; and (b) accounts of terminated or transferred users;
- granting access to the system based on: (a) a valid access authorization; (b) intended system usage; and (c) other attributes as required by the organization or associated missions/business functions;

the organization reviews information system accounts in accordance with the frequency specified in Implementation Standard 1.

the organization meets all the requirements specified in the applicable implementation standard(s).

Assessment Methods And Objects

Examine: Access control policy; procedures addressing account management; security plan; list of active system accounts along with the name of the individual associated with each account; list of guest/anonymous and temporary accounts along with the name of the individual associated with the each account and the date the account expires; lists of recently transferred, separated, or terminated employees; list of recently disabled information system accounts along with the name of the individual associated with each account; system-generated records with user IDs and last login date; other relevant documents or records.

AC-2(3) – Enhancement (Low)		
Control The information system automatically disables inactive accounts after three hundred sixty-five (365) days.		
Applicability: All	**Reference(s):**	**Related Controls Requirement(s):** IA-4.Std.1
ASSESSMENT PROCEDURE: AC-2(3).1		
Assessment Objective Determine if: the organization defines in the security plan, explicitly or by reference, a time period after which the information system disables inactive accounts; the information system automatically disables inactive accounts after organization-defined time period.		
Assessment Methods And Objects **Examine:** Procedures addressing account management; security plan; information system design documentation; information system configuration settings and associated documentation; information system-generated list of last login dates; information system-generated list of active accounts; information system audit records; other relevant documents or records.		
AC-2(7) – Enhancement (Low)		
Control The organization: (a) Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles; (b) Tracks and monitors privileged role assignments; and (c) Inspects administrator groups, root accounts and other system related accounts on demand, but at least once every thirty (30) days to ensure that unauthorized accounts have not been created.		
Guidance Privileged roles include, for example, key management, network and system administration, database administration, web administration.		
Applicability: All	**Reference(s):**	**Related Controls Requirement(s):**
ASSESSMENT PROCEDURE: AC-2(7).1		
Assessment Objective Determine if: the organization establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles; the organization tracks and monitors privileged role assignments; the organization inspects administrator groups, root accounts and other system related accounts on demand, but at least once during the specified period to ensure that unauthorized accounts have not been created.		
Assessment Methods And Objects **Examine:** Procedures addressing account management; information system design documentation; information system configuration settings and associated documentation; information system-generated list of privileged user accounts and associated role; information system audit records; audit tracking and monitoring reports; other relevant documents or records.		

AC-3 – Access Enforcement (Low)

Control

The information system enforces approved authorizations for logical access to the system in accordance with applicable policy.

Implementation Standard(s)

1. If encryption is used as an access control mechanism it must meet CMS approved (FIPS 140-2 compliant and a NIST validated module) encryption standards (see SC-13).
2. If e-authentication is utilized in connection to access enforcement, refer to ARS Appendix D: E-authentication Standard.
3. Configure operating system controls to disable public "write" access to files, objects, and directories that may directly impact system functionality and/or performance.

Guidance

Access control policies (e.g., identity-based policies, role-based policies, attribute-based policies) and access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) are employed by organizations to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system. In addition to enforcing authorized access at the information-system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. Consideration is given to the implementation of an audited, explicit override of automated mechanisms in the event of emergencies or other serious events. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used is FIPS 140-2 (as amended) compliant.
Encryption as access enforcement extends to all government and non-government furnished desktop computers that store sensitive information. While encryption is the preferred technical solution for protection of sensitive information on all desktop computers, adequate physical security controls and other management controls are acceptable mitigations for the protection of desktop computers with the approval of the CIO or his/her designated representative. Mechanisms implemented by AC-3 are configured to enforce authorizations determined by other security controls.

Applicability: All	**Reference(s):** FISCAM: AC-3, AC-4, AS-1, AS-2, AS-3, AS-4, BP-2, BP-4, CM-3, DA-1, IN-2; HIPAA: 164.310(a)(2)(iii), 164.312(a)(1); IRS-1075: 5.6.3.2#2.2, 5.6.3.3#3	**Related Controls Requirement(s):** SC-13

ASSESSMENT PROCEDURE: AC-3.1

Assessment Objective

Determine if:
the information system enforces approved authorizations for logical access to the system in accordance with applicable policy.

the organization meets all the requirements specified in the applicable implementation standard(s).

Assessment Methods And Objects

Examine: Access control policy; procedures addressing access enforcement; information system configuration settings and associated documentation; list of approved authorizations (user privileges); information system audit records; other relevant documents or records.

AC-3(1) – Enhancement (Low)

Control

[Withdrawn: Incorporated into AC-6].

AC-5 – Separation of Duties (Low)

Control

The organization:
a. Separates duties of individuals as necessary, to prevent malevolent activity without collusion;
b. Documents separation of duties; and
c. Implements separation of duties through assigned information system access authorizations.

Implementation Standard(s)

1. Ensure that audit functions are not performed by security personnel responsible for administering access control.
2. Maintain a limited group of administrators with access based upon the users' roles and responsibilities.

3. Ensure that critical mission functions and information system support functions are divided among separate individuals.
4. Ensure that information system testing functions (i.e., user acceptance, quality assurance, information security) and production functions are divided among separate individuals or groups.

Guidance

Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, configuration management, quality assurance and testing, network security); (iii) security personnel who administer access control functions do not administer audit functions; and (iv) different administrator accounts for different roles. Access authorizations defined in this control are implemented by control AC-3.

Applicability: All	**Reference(s):** FISCAM: AS-1, AS-2, AS-3, AS-4, BP-4, SD-1, SD-2; HIPAA: 164.308(a)(4)(ii)(A); IRS-1075: 5.6.2.3#1, 5.6.3.2#3.1, 5.6.3.3#3	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AC-5.1

Assessment Objective

Determine if:
the organization separates duties of individuals as necessary, to prevent malevolent activity without collusion;

the organization documents separation of duties;

the organization implements separation of duties through assigned information system access authorizations.

the organization meets all the requirements specified in the applicable implementation standard(s).

Assessment Methods And Objects

Examine: Access control policy; procedures addressing divisions of responsibility and separation of duties; information system configuration settings and associated documentation; list of divisions of responsibility and separation of duties; information system audit records; other relevant documents or records.

AC-6 – Least Privilege (Low)

Control

The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with CMS missions and business functions.

Implementation Standard(s)

1. Disable all file system access not explicitly required for system, application, and administrator functionality.
2. Contractors must be provided with minimal system and physical access, and must agree to and support the CMS security requirements. The contractor selection process must assess the contractor's ability to adhere to and support CMS security policy.
3. Restrict the use of database management utilities to only authorized database administrators.
4. Disable all system and removable media boot access unless it is explicitly authorized by the CIO for compelling operational needs. If authorized, boot access is password protected.

Guidance

The access authorizations defined in this control are largely implemented by control AC-3. The organization employs the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to CMS operations and assets, individuals, other organizations, and the Nation.

Applicability: All	**Reference(s):** FISCAM: AC-3, AC-4, AS-2, AS-3; HIPAA: 164.308(a)(3)(i), 164.308(a)(4)(ii)(A); HSPD 7: D(10); IRS-1075: 5.6.2.3#1, 5.6.3.2#3.2	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AC-6.1		
Assessment Objective Determine if: the organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. the organization meets all the requirements specified in the applicable implementation standard(s). **Assessment Methods And Objects** **Examine:** Access control policy; procedures addressing least privilege; list of assigned access authorizations (user privileges); information system configuration settings and associated documentation; information system audit records; other relevant documents or records.		
AC-6(1) – Enhancement (Low)		
Control The organization explicitly authorizes access to privileged functions (e.g., system-level software, administrator tools, scripts, utilities) deployed in hardware, software, and firmware; and security relevant information is restricted to explicitly authorized individuals.		
Guidance Establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters are examples of security functions. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users.		
Applicability: All	**Reference(s):**	**Related Controls Requirement(s):**
ASSESSMENT PROCEDURE: AC-6(1).1		
Assessment Objective Determine if: the organization defines the security functions (deployed in hardware, software, and firmware) and security-relevant information for which access must be explicitly authorized; the organization explicitly authorizes access to the organization-defined security functions and security-relevant information. **Assessment Methods And Objects** **Examine:** Access control policy; procedures addressing least privilege; list of security functions and security-relevant information for which access must be explicitly authorized; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.		
AC-6(2) – Enhancement (Low)		
Control The organization requires that users of information system accounts, or roles, with access to administrator accounts or security functions, use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions.		
Guidance This control enhancement is intended to limit exposure due to operating from within a privileged account or role. The inclusion of role is intended to address those situations where an access control policy such as Role Based Access Control (RBAC) is being implemented and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account. Audit of privileged activity may require physical separation employing information systems on which the user does not have privileged access.		
Applicability: All	**Reference(s):**	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AC-6(2).1

Assessment Objective

Determine if:
the organization defines the security functions or security-relevant information to which users of information system accounts, or roles, have access;

the organization requires that users of information system accounts, or roles, with access to organization-defined security functions or security-relevant information, use non-privileged accounts, or roles, when accessing other system functions;

the organization, if deemed feasible, audits any use of privileged accounts, or roles, with access to organization-defined security functions or security-relevant information, when accessing other system functions.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing least privilege; list of system-generated security functions or security-relevant information assigned to information system accounts or roles; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

AC-7 – Unsuccessful Login Attempts (Low)

Control

The information system:
a. Enforces the limit of consecutive invalid login attempts by a user specified in Implementation Standard 1 during the time period specified in Implementation Standard 1; and
b. Automatically disables or locks the account/node until released after the time period specified in Implementation Standard 1 when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection.

Implementation Standard(s)

1. Configure the information system to disable access for at least five (5) minutes after three (3) failed log-on attempts by a user during a five (5) minute time period.

Guidance

Due to the potential for denial of service, automatic lockouts initiated by the information system are usually temporary and automatically release after a predetermined time period established by the organization. If a delay algorithm is selected, the organization may chose to employ different algorithms for different information system components based on the capabilities of those components. Response to unsuccessful login attempts may be implemented at both the operating system and the application levels. This control applies to all accesses other than those accesses explicitly identified and documented by the organization in AC-14.

Applicability: All	**Reference(s):** FISCAM: AC-2; IRS-1075: 5.6.3.2#4.1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AC-7.1

Assessment Objective

Determine if:
the organization defines in the security plan, explicitly or by reference, the maximum number of consecutive invalid login attempts to the information system by a user and the time period in which the consecutive invalid login attempts occur;

the information system enforces the organization-defined limit of consecutive invalid login attempts by a user during the organization-defined time period;

the organization defines action to be taken by the system when the maximum number of unsuccessful login attempts is exceeded as:
- lock out the account/node for a specified time period;
- lock out the account/note until released by an administrator; or
- delay the next login prompt according to organization-defined delay algorithm;

the information system either automatically locks the account/node for the organization-defined time period, locks the account/node until released by an administrator, or delays next login prompt for the organization-defined delay period when the maximum number of unsuccessful login attempts is exceeded;

the information system performs the organization-defined actions when the maximum number of unsuccessful login attempts is exceeded regardless of whether the login occurs via a local or network connection.

the organization meets all the requirements specified in the applicable implementation standard(s).

Assessment Methods And Objects

Examine: Access control policy; procedures addressing unsuccessful login attempts; security plan; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

AC-8 – System Use Notification (Low)

Control

The information system:
a. Displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The approved banner for CMS information systems is:
- You are accessing a U.S. Government information system, which includes: (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.
- Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.
- By using this information system, you understand and consent to the following:
  * You have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system. At any time, and for any lawful Government purpose, the Government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system.
  * Any communication or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose.

b. Retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system; and
c. For publicly accessible systems: (i) displays the system use information when appropriate, before granting further access; (ii) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) includes in the notice given to public users of the information system, a description of the authorized uses of the system.

Guidance

The warning banner language has very important legal implications for CMS and its information system resources. Should content need to be added to this banner, submit the modified warning banner language to the CMS CIO for review and approval prior to implementation. If an information system has character limitations related to the warning banner display, the CMS CIO can provide an abbreviated warning banner version. If this banner is inconsistent with any directives, policies, regulations, or standards, notify the CMS CIO immediately.
All CMS information system computers and network devices under CMS control, prominently display the notice and consent banner immediately upon users' authentication to the system, including, but not limited to, web sites, web pages where substantial personal information from the public is collected, ftp, telnet, or other services accessed.
System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. System use notification is intended only for information system access that includes an interactive login interface with a human user and is not intended to require notification when an interactive interface does not exist.

Applicability: All	**Reference(s):** FISCAM: AC-1; IRS-1075: 5.1#1.3, 5.6.3.2#4.2	**Related Controls Requirement(s):** SI-4

ASSESSMENT PROCEDURE: AC-8.1

Assessment Objective

Determine if:
the information system displays the CMS-approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:
- users are accessing a U.S. Government information system;
- system usage may be monitored, recorded, and subject to audit;
- unauthorized use of the system is prohibited and subject to criminal and civil penalties;
- use of the system indicates consent to monitoring and recording;

the information system retains the notification message or banner on the screen until the user takes explicit actions to log on to or further access the information system;

the system use notification message remains on the screen until the user takes explicit actions to log on to the information system.

Assessment Methods And Objects

Examine: Access control policy; privacy and security policies; procedures addressing system use notification; documented approval of information system use notification messages or banners; information system notification messages; information system configuration settings and associated documentation; information system audit records for user acceptance of notification message or banner; other relevant documents or records.

ASSESSMENT PROCEDURE: AC-8.2

Assessment Objective

Determine if:
the information system (for publicly accessible systems) displays the system use information when appropriate, before granting further access;

the information system (for publicly accessible systems) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities;

the information system (for publicly accessible systems) includes in the notice given to public users of the information system, a description of the authorized uses of the information system.

Assessment Methods And Objects

Examine: Access control policy; privacy and security policies; procedures addressing system use notification; documented approval of information system use notification messages or banners; information system notification messages; information system configuration settings and associated documentation; other relevant documents or records.

AC-12 – Session Termination (Low)

Control

[Withdrawn: Incorporated into SC-10].

AC-13 – Supervision and Review--Access Control (Low)

Control

[Withdrawn: Incorporated into AC-2 and AU-6].

AC-14 – Permitted Actions without Identification or Authentication (Low)

Control

The organization:
a. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication; and
b. Configures Information systems to permit public access only to the extent necessary to accomplish mission objectives, without first requiring individual identification and authentication.

Guidance

This control is intended for public websites and other publicly available systems. It is intended for those specific instances where an organization determines that no identification and authentication is required; it is not, however, mandating that such instances exist in given information system. The organization may allow a limited number of user actions without identification and authentication (e.g., when individuals access public websites or other publicly accessible federal information systems such as http://www.usa.gov). Organizations also identify any actions that normally require identification or authentication but may under certain circumstances (e.g., emergencies), allow identification or authentication mechanisms to be bypassed. Such bypass may be, for example, via a software-readable physical switch that commands bypass of the login functionality and is protected from accidental or unmonitored use. This control does not apply to situations where identification and authentication have already occurred and are not being repeated, but rather to situations where identification and/or authentication have not yet occurred.

Applicability: All	**Reference(s):** FISCAM: AC-2, AC-3, AS-2	**Related Controls Requirement(s):** IA-2

ASSESSMENT PROCEDURE: AC-14.1

Assessment Objective

Determine if:
the organization identifies specific user actions that can be performed on the information system without identification or authentication;

the organization documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing permitted actions without identification and authentication; information system configuration settings and associated documentation; security plan; list of information system actions that can be performed without identification and authentication; information system audit records; other relevant documents or records.

AC-15 – Automated Marking (Low)

Control

[Withdrawn: Incorporated into MP-3].

AC-17 – Remote Access (Low)

Control

Remote access for privileged functions shall be permitted only for compelling operational needs, shall be strictly controlled, and must be explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization:
a. Documents allowed methods of remote access to the information system;
b. Establishes usage restrictions and implementation guidance for each allowed remote access method;
c. Monitors for unauthorized remote access to the information system;
d. Authorizes remote access to the information system prior to connection; and
e. Enforces requirements for remote connections to the information system.

Implementation Standard(s)

1. Require callback capability with re-authentication to verify connections from authorized locations when the Medicare Data Communications Network (MDCN) or Multi Protocol Label Switching (MPLS) service network cannot be used.
2. If e-authentication is implemented as a remote access solution or associated with remote access, refer to ARS Appendix D: E-authentication Standard.

Guidance

This control requires explicit authorization prior to allowing remote access to a CMS information system without specifying a specific format for that authorization. For example, while the organization may deem it appropriate to use a system interconnection agreement to authorize a given remote access, such agreements are not required by this control. Remote access is any access to a CMS information system by a user (or process acting on behalf of a user) communicating through an external network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless (see AC-18 for wireless access). A virtual private network (VPN) when adequately provisioned with appropriate security controls, is considered an internal network (i.e., the organization establishes a network connection between organization-controlled endpoints in a manner that does not require the organization to depend on external networks to protect the confidentiality or integrity of information transmitted across the network). Remote access controls are applicable to CMS information systems other than public web servers or systems specifically designed for public access. Enforcing access restrictions associated with remote connections is accomplished by control AC-3.

Applicability: All	**Reference(s):** FISCAM: AC-1, AC-4; IRS-1075: 5.6.3.2#5, 5.7.1#1	**Related Controls Requirement(s):** IA-2, SC-9

ASSESSMENT PROCEDURE: AC-17.1

Assessment Objective

Determine if:
the organization documents allowed methods of remote access to the information system;

the organization establishes usage restrictions and implementation guidance for each allowed remote access method;

the organization monitors for unauthorized remote access to the information system;

the organization authorizes remote access to the information system prior to connection;

the organization enforces requirements for remote connections to the information system.

the organization meets all the requirements specified in the applicable implementation standard(s).

Assessment Methods And Objects

Examine: Access control policy; procedures addressing remote access to the information system; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

AC-17(7) – Enhancement (Low)

Control

The organization ensures that remote sessions used for remote administration employ additional security measures (e.g., Secure Shell [SSH], Virtual Private Networking [VPN] with blocking mode enabled) and the CMS-approved encryption standard (see SC-13).

Guidance

Additional security measures are typically above and beyond standard bulk or session layer encryption (e.g., Secure Shell [SSH], Virtual Private Networking [VPN] with blocking mode enabled).

Applicability: All	**Reference(s):**	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AC-17(7).1

Assessment Objective

Determine if:
the organization defines the security functions and security-relevant information that can be accessed using remote sessions;

the organization defines the additional security measures to be employed for remote sessions used to access organization-defined security functions and security-relevant information;

the organization employs the CMS-approved encryption standard (see SC-13) for remote sessions used to access organization-defined security functions and security-relevant information;

the organization audits remote sessions for accessing organization-defined security functions and security-relevant information, if required by the control.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing remote access to the information system; information system design documentation; information system configuration settings and associated documentation; information system audit records (if auditing is required); other relevant documents or records.

AC-18 – Wireless Access (Low)

Control

The organization prohibits the installation of wireless access points (WAP) to CMS information systems unless explicitly authorized, in writing, by the CMS CIO or his/her designated representative. If authorized, the organization:
a. Monitors for unauthorized wireless access to the information system; and
b. Enforces requirements for wireless connections to the information system.

Implementation Standard(s)

1. If wireless access is explicitly approved, wireless device service set identifier broadcasting is disabled and the following wireless access controls are implemented:
(a) Encryption protection is enabled;
(b) Access points are placed in secure areas;
(c) Access points are shut down when not in use (i.e., nights, weekends);

(d) A firewall is implemented between the wireless network and the wired infrastructure;
(e) MAC address authentication is utilized;
(f) Static IP addresses, not DHCP, is utilized;
(g) Personal firewalls are utilized on all wireless clients;
(h) File sharing is disabled on all wireless clients;
(i) Intrusion detection agents are deployed on the wireless side of the firewall; and
(j) Wireless activity is monitored and recorded, and the records are reviewed on a regular basis.

Guidance

Wireless technologies include, but are not limited to, microwave, satellite, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., EAP/TLS, PEAP), which provide credential protection and mutual authentication. In certain situations, wireless signals may radiate beyond the confines and control of organization-controlled facilities.

Applicability: All	**Reference(s):** FISCAM: AC-1, AC-4	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AC-18.1

Assessment Objective

Determine if:
the organization establishes usage restrictions and implementation guidance for wireless access;

the organization monitors for unauthorized wireless access to the information system;

the organization authorizes wireless access to the information system prior to connection;

the organization enforces requirements for wireless connections to the information system.

the organization meets all the requirements specified in the applicable implementation standard(s).

Assessment Methods And Objects

Examine: Access control policy; procedures addressing wireless implementation and usage (including restrictions); activities related to wireless monitoring, authorization, and enforcement; information system audit records; other relevant documents or records.

AC-19 – Access Control for Mobile Devices (Low)

Control

The organization prohibits the connection of portable and mobile devices (e.g., notebook computers, personal digital assistants [PDA], cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) to CMS information systems unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization:
a. Employs an approved method of cryptography (see SC-13) to protect information residing on portable and mobile information devices, and utilizes whole-disk encryption solution for laptops;
b. Monitors for unauthorized connections of mobile devices to CMS information systems;
c. Enforces requirements for the connection of mobile devices to CMS information systems;
d. Disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction;
e. Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures; and
f. Protects the storage and transmission of information on portable and mobile information devices with activities such as scanning the devices for malicious code, virus protection software.

Guidance

Mobile devices include portable storage media (e.g., USB memory sticks, external hard disk drives) and portable computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). Organization-controlled mobile devices include those devices for which the organization has the authority to specify and the ability to enforce specific security requirements. Usage restrictions and implementation guidance related to mobile devices include, for example, configuration management, device identification and authentication, implementation of mandatory protective software

(e.g., malicious code detection, firewall), scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Examples of information system functionality that provide the capability for automatic execution of code are AutoRun and AutoPlay.
Organizational policies and procedures for mobile devices used by individuals departing on and returning from travel include, for example, determining which locations are of concern, defining required configurations for the devices, ensuring that the devices are configured as intended before travel is initiated, and applying specific measures to the device after travel is completed. Specially configured mobile devices include, for example, computers with sanitized hard drives, limited applications, and additional hardening (e.g., more stringent configuration settings). Specified measures applied to mobile devices upon return from travel include, for example, examining the device for signs of physical tampering and purging/reimaging the hard disk drive. Protecting information residing on mobile devices is covered in the media protection family.

Applicability: All	**Reference(s):** FISCAM: AC-1; IRS-1075: 4.6#1	**Related Controls Requirement(s):** MP-4, MP-5

ASSESSMENT PROCEDURE: AC-19.1

Assessment Objective

Determine if:
the organization prohibits the connection of portable and mobile devices to the information system unless explicitly authorized, in writing, by the CIO;

if authorized, the organization employs an approved method of cryptography (see SC-13) to protect information residing on portable and mobile information devices, and utilizes whole-disk encryption solution for laptops;

if authorized, the organization monitors for unauthorized connections of mobile devices to organizational information systems;

if authorized, the organization enforces requirements for the connection of mobile devices to organizational information systems;

if authorized, the organization disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction;

if authorized, the organization issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures;

if authorized, the organization defines the inspection and preventative measures to be applied to mobile devices returning from locations that the organization deems to be of significant risk;

if authorized, the organization applies organization-defined inspection and preventative measures to mobile devices returning from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.

Assessment Methods And Objects

Examine: Access control policy; procedures addressing access control for portable and mobile devices; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

AC-20 – Use of External Information Systems (Low)

Control

The organization prohibits the use of external information systems, including but not limited to, Internet kiosks, personal desktop computers, laptops, tablet personal computers, personal digital assistant (PDA) devices, cellular telephones, facsimile machines, and equipment available in hotels or airports to store, access, transmit, or process CMS sensitive information, unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization establishes strict terms and conditions for their use. The terms and conditions shall address, at a minimum:
a. The types of applications that can be accessed from external information systems;
b. The maximum FIPS 199 security category of information that can be processed, stored, and transmitted;
c. How other users of the external information system will be prevented from accessing federal information;
d. The use of virtual private networking (VPN) and firewall technologies;
e. The use of and protection against the vulnerabilities of wireless technologies;
f. The maintenance of adequate physical security controls;
g. The use of virus and spyware protection software; and
h. How often the security capabilities of installed software are to be updated.

Implementation Standard(s)

1. Instruct all personnel working from home to implement fundamental security controls and practices, including passwords, virus protection, and personal firewalls. Limit remote access only to information resources required by home users to complete job duties. Require that any government-owned equipment be used only for business purposes by authorized employees.

Guidance

External information systems are information systems or components of information systems that are outside of the authorization boundary established by the organization and for which the organization typically has no direct supervision and authority over the application of required security controls or the assessment of security control effectiveness. External information systems include, but are not limited to: (i) personally owned information systems (e.g., computers, cellular telephones, or personal digital assistants); (ii) privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, or airports); (iii) information systems owned or controlled by nonfederal governmental organizations; and (iv) federal information systems that are not owned by, operated by, or under the direct supervision and authority of the organization. For some external systems, in particular those systems operated by other federal agencies, including organizations subordinate to CMS, the trust relationships that have been established between those organizations and the originating organization may be such, that no explicit terms and conditions are required. In effect, the information systems of these organizations would not be considered external. These situations typically occur when, for example, there is some pre-existing sharing or trust agreement (either implicit or explicit) established between federal agencies and/or organizations subordinate to those agencies, or such trust agreements are specified by applicable laws, Executive Orders, directives, or policies.

This control does not apply to the use of external information systems to access public interfaces to CMS information systems and information (e.g., individuals accessing federal information through www.medicare.gov). The organization establishes terms and conditions for the use of external information systems in accordance with CMS security policies and procedures. The terms and conditions address as a minimum; (i) the types of applications that can be accessed on the CMS information system from the external information system; and (ii) the maximum security categorization of information that can be processed, stored, and transmitted on the external information system. This control defines access authorizations enforced by AC-3, rules of behavior requirements enforced by PL-4, and session establishment rules enforced by AC-17.

Applicability: All	**Reference(s):** FISCAM: SM-7; IRS-1075: 4.7.2#1, 4.7.3#1.1, 5.7#1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AC-20.1

Assessment Objective

Determine if:

the organization prohibits the use of external information systems to store, access, transmit, or process sensitive information unless explicitly authorized, in writing, by the CIO;

if authorized, the organization identifies individuals authorized to:
- access the information system from the external information systems;
- process, store, and/or transmit organization-controlled information using the external information systems;

if authorized, the terms and conditions address, at a minimum:
- the types of applications that can be accessed from external information systems;
- the maximum FIPS 199 security category of information that can be processed, stored, and transmitted;
- how other users of the external information system will be prevented from accessing federal information;
- the use of virtual private networking (VPN) and firewall technologies;
- the use of and protection against the vulnerabilities of wireless technologies;
- the maintenance of adequate physical security controls;
- the use of virus and spyware protection software; and
- how often the security capabilities of installed software are to be updated.

the organization meets all the requirements specified in the applicable implementation standard(s).

Assessment Methods And Objects

Examine: Access control policy; procedures addressing the use of external information systems; external information systems terms and conditions; list of types of applications accessible from external information systems; maximum security categorization for information processed, stored, or transmitted on external information systems; information system configuration settings and associated documentation; other relevant documents or records.

AC-22 – Publicly Accessible Content (Low)		
Control The organization: a. Designates individuals authorized to post information onto a CMS information system that is publicly accessible; b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the CMS information system; d. Reviews the content on the publicly accessible CMS information system for nonpublic information monthly; and e. Removes nonpublic information from the publicly accessible CMS information system, if discovered.		
Guidance Nonpublic information is any information for which the general public is not authorized access in accordance with federal laws, Executive Orders, directives, policies, regulations, standards, or guidance. Information protected under the Privacy Act and vendor proprietary information are examples of nonpublic information. This control addresses posting information on a CMS information system that is accessible to the general public, typically without identification or authentication. The posting of information on non-CMS information systems is covered by appropriate organizational policy.		
Applicability: All	**Reference(s):**	**Related Controls Requirement(s):**
ASSESSMENT PROCEDURE: AC-22.1		
Assessment Objective Determine if: the organization designates individuals authorized to post information onto a CMS information system that is publicly accessible; the organization trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; the organization reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the CMS information system; the organization reviews the content on the publicly accessible CMS information system for nonpublic information monthly; the organization removes nonpublic information from the publicly accessible CMS information system, if discovered.		
Assessment Methods And Objects **Examine:** Access control policy; procedures addressing publicly accessible content; list of users authorized to post publicly accessible content on organizational information systems; training materials and/or records; records of publicly accessible information reviews; records of response to nonpublic information on public websites; system audit logs; security awareness training records; other relevant documents or records.		

Awareness and Training (AT) – *Operational*

AT-1 – Security Awareness and Training Policy and Procedures (Low)

Control

The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:
a. A formal, documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.

Guidance

This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the security awareness and training family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The security awareness and training policy can be included as part of the general information security policy for the organization. Security awareness and training procedures can be developed for the security program in general and for a particular CMS information system, when required. The organizational risk management strategy is a key factor in the development of the security awareness and training policy.

Applicability: All	**Reference(s):** FISCAM: AC-6, AS-1, SM-1, SM-3, SM-7; IRS-1075: 5.6.2.7#1.1-2, 6.1#1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AT-1.1

Assessment Objective

Determine if:
the organization develops and formally documents security awareness and training policy;

the organization security awareness and training policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities, and compliance;

the organization disseminates formal documented security awareness and training policy to elements within the organization having associated security awareness and training roles and responsibilities;

the organization develops and formally documents security awareness and training procedures;

the organization security awareness and training procedures facilitate implementation of the security awareness and training policy and associated security awareness and training controls;

the organization disseminates formal documented security awareness and training procedures to elements within the organization having associated security awareness and training roles and responsibilities;

the organization reviews/updates the security awareness and training policy and procedures within every three hundred sixty-five (365) days.

Assessment Methods And Objects

Examine: Security awareness and training policy and procedures; other relevant documents or records.

AT-2 – Security Awareness (Low)

Control

The organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users prior to accessing any system's information, when required by system changes, and within every three hundred sixty-five (365) days thereafter.

Guidance

The organization determines the appropriate content of security awareness training and security awareness techniques based on the specific requirements of the organization and the CMS information systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security as it relates to CMS' information security program. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events.

Applicability: All	**Reference(s):** FISCAM: AC-6, SM-4; HIPAA: 164.308(a)(5)(i); IRS-1075: 5.6.2.7#1.3	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AT-2.1

Assessment Objective

Determine if:
the organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users and when required by system changes;

the organization defines in the security plan, explicitly or by reference, the frequency of refresher security awareness training and the frequency is at least annually;

the organization provides refresher security awareness training in accordance with the organization-defined frequency.

Assessment Methods And Objects

Examine: Security awareness and training policy; procedures addressing security awareness training implementation; appropriate codes of federal regulations; security awareness training curriculum; security awareness training materials; security plan; training records; other relevant documents or records.

AT-3 – Security Training (Low)

Control

The organization provides role-based security-related training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) refresher training within every three hundred sixty-five (365) days thereafter.

Implementation Standard(s)

1. Require personnel with significant information security roles and responsibilities to undergo appropriate information system security training prior to authorizing access to CMS networks, systems, and/or applications; when required by system changes; and refresher training within every three hundred sixty-five (365) days thereafter.

Guidance

The organization determines the appropriate content of security training based on assigned roles and responsibilities and the specific requirements of CMS and the information systems to which personnel have authorized access. In addition, the organization provides information system managers, system and network administrators, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software, adequate security-related technical training to perform their assigned duties. Organizational security training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. The organization also provides the training necessary for these individuals to carry out their responsibilities related to operations security within the context of CMS' information security program.

Applicability: All	**Reference(s):** FISCAM: AS-1, SM-4; IRS-1075: 5.6.2.7#1.4	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AT-3.1

Assessment Objective

Determine if:
the organization provides role-based security-related training before authorizing access to the system or performing assigned duties, and when required by system changes;

the organization provides role-based security-related refresher training within every three hundred sixty-five (365) days thereafter.

the organization meets all the requirements specified in the applicable implementation standard(s).

Assessment Methods And Objects

Examine: Security awareness and training policy; procedures addressing security training implementation; codes of federal regulations; security training curriculum; security training materials; security plan; training records; other relevant documents or records.

AT-4 – Security Training Records (Low)

Control

The organization:
a. Documents and monitors individual CMS information system security training activities including basic security awareness training and specific information system security training; and
b. Retains individual training records for three (3) years.

Guidance

Procedures and training implementation should:
(a) Identify employees with significant information security responsibilities and provide role-specific training in accordance with National Institute of Standards and Technology (NIST) standards and guidance:
1) All users of CMS information systems must be exposed to security awareness materials at least annually. Users of CMS information systems include employees, contractors, students, guest researchers, visitors, and others who may need access to CMS information systems and applications.
2) Executives must receive training in information security basics and policy level training in security planning and management.
3) Program and functional managers must receive training in information security basics; management and implementation level training in security planning and system/application security management; and management and implementation level training in system/ application life cycle management, risk management, and contingency planning.
4) Chief Information Officers (CIOs), IT security program managers, auditors, and other security-oriented personnel (e.g., system and network administrators, and system/application security officers) must receive training in information security basics and broad training in security planning, system and application security management, system/application life cycle management, risk management, and contingency planning.
5) IT function management and operations personnel must receive training in information security basics; management and implementation level training in security planning and system/application security management; and management and implementation level training in system/application life cycle management, risk management, and contingency planning.
(b) Provide the CMS information systems security awareness material/exposure outlined in NIST guidance on IT security awareness and training to all new employees before allowing them access to the systems.
(c) Provide information systems security refresher training for employees as frequently as determined necessary, based on the sensitivity of the information that the employees use or process.
(d) Provide training whenever there is a significant change in the information system environment or procedures or when an employee enters a new position that requires additional role-specific training.

Applicability: All	**Reference(s):** FISCAM: AS-1, SM-4; IRS-1075: 6.2#1.3	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AT-4.1

Assessment Objective

Determine if:
the organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training;

the organization retains individual training records in accordance with the organization-defined time period.

Assessment Methods And Objects

Examine: Security awareness and training policy; procedures addressing security training records; security awareness and training records; other relevant documents or records.

Audit and Accountability (AU) – *Technical*

AU-1 – Audit and Accountability Policy and Procedures (Low)

Control

The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:
a. A formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.

Guidance

This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the audit and accountability family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The audit and accountability policy can be included as part of the general information security policy for the organization. Audit and accountability procedures can be developed for the security program in general and for a particular CMS information system, when required. The organizational risk management strategy is a key factor in the development of the audit and accountability policy.

Applicability: All	**Reference(s):** FISCAM: AS-1, AS-2, SM-1, SM-3; IRS-1075: 5.6.3.3#1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AU-1.1

Assessment Objective

Determine if:
the organization develops and formally documents audit and accountability policy;

the organization audit and accountability policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented audit and accountability policy to elements within the organization having associated audit and accountability roles and responsibilities;

the organization develops and formally documents audit and accountability procedures;

the organization audit and accountability procedures facilitate implementation of the audit and accountability policy and associated audit and accountability controls;

the organization disseminates formal documented audit and accountability procedures to elements within the organization having associated audit and accountability roles and responsibilities.

the organization reviews/updates the audit and accountability policy and procedures within every three hundred sixty-five (365) days.

Assessment Methods And Objects

Examine: Audit and accountability policy and procedures; other relevant documents or records.

AU-2 – Auditable Events (Low)

Control

The organization:
a. Determines, based on a risk assessment and CMS mission/business needs, that the information system must be capable of auditing the list of auditable events specified in the Implementation Standards;
b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of

auditable events; and
c. Determines, based on current threat information and ongoing assessment of risk, which events require auditing on a continuous basis and which events require auditing in response to specific situations.

Implementation Standard(s)

1. Generate audit records for the following events:
(a) User account management activities,
(b) System shutdown,
(c) System reboot,
(d) System errors,
(e) Application shutdown,
(f) Application restart,
(g) Application errors,
(h) File creation, and
(i) File deletion.
2. Enable logging for perimeter devices, including firewalls and routers.
(a) Log packet screening denials originating from untrusted networks,
(b) Packet screening denials originating from trusted networks,
(c) User account management,
(d) Modification of packet filters,
(e) Application errors,
(f) System shutdown and reboot, and
(g) System errors.
3. Verify that proper logging is enabled in order to audit administrator activities.

Guidance

The purpose of this control is for the organization to identify events which need to be auditable as significant and relevant to the security of the information system; giving an overall system requirement in order to meet ongoing and specific audit needs. To balance auditing requirements with other information system needs, this control also requires identifying that subset of auditable events that are to be audited at a given point in time. For example, the organization may determine that the information system must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the extreme burden on system performance. In addition, audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems.

Applicability: All	**Reference(s):** FISCAM: AC-3, AC-4, AC-5, AS-2, DA-1; HIPAA: 164.308(a)(5)(ii)(C), 164.312(b); IRS-1075: 5.6.3.3#2.1	**Related Controls Requirement(s):** AU-4

ASSESSMENT PROCEDURE: AU-2.1

Assessment Objective

Determine if:
the organization determines, based on a risk assessment and CMS mission/business needs, that the information system must be capable of auditing the list of auditable events specified in the Implementation Standards;

the organization coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and help guide the selection of auditable events;

the organization provides a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents;

the organization defines in the security plan, explicitly or by reference, information system auditable events;

the organization defines the subset of auditable events defined in (a) that are to be audited within the information system and (b) the frequency of (or situation requiring) auditing for each identified event;

the organization determines, based on current threat information and ongoing assessment of risk, the subset of auditable events defined in (a) to be audited within the information

system, and (b) the frequency of (or situation requiring) auditing for each identified event.

the organization meets all the requirements specified in the applicable implementation standard(s).

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing auditable events; security plan; information system configuration settings and associated documentation; information system audit records; list of information system auditable events; other relevant documents or records.

AU-2(1) – Enhancement (Low)

Control

[Withdrawn: Incorporated into AU-12].

AU-2(2) – Enhancement (Low)

Control

[Withdrawn: Incorporated into AU-12].

AU-3 – Content of Audit Records (Low)

Control

The information system produces audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.

Guidance

Audit record content that may be necessary to satisfy the requirement of this control, includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

Applicability: All	**Reference(s):** FISCAM: AC-5, AS-2, DA-1; IRS-1075: 5.6.3.3#3	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AU-3.1

Assessment Objective

Determine if the information system produces audit records that contain sufficient information to, at a minimum, establish:
- what type of event occurred;
- when (date and time) the event occurred;
- where the event occurred;
- the source of the event;
- the outcome (success or failure) of the event;
- the identity of any user/subject associated with the event.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing content of audit records; list of organization-defined auditable events; information system audit records; information system incident reports; other relevant documents or records.

AU-4 – Audit Storage Capacity (Low)

Control

The organization allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.

Guidance

The organization considers the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity.

Applicability: All	**Reference(s):** FISCAM: AC-5; IRS-1075: 5.6.3.3#4	**Related Controls Requirement(s):** AU-2, AU-

		5, AU-6, AU-7, SI-4

ASSESSMENT PROCEDURE: AU-4.1

Assessment Objective

Determine if:
the organization allocates audit record storage capacity;

the organization configures auditing to reduce the likelihood of audit record storage capacity being exceeded.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit storage capacity; information system design documentation; organization-defined audit record storage capacity for information system components that store audit records; list of organization-defined auditable events; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

AU-5 – Response to Audit Processing Failures (Low)

Control

The information system:
a. Alerts designated organizational officials in the event of an audit processing failure; and
b. Takes the following additional actions in response to an audit failure or audit storage capacity issue:
- Shutdown the information system,
- Stop generating audit records, or
- Overwrite the oldest records, in the case that storage media is unavailable.

Guidance

Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

Applicability: All	**Reference(s):** FISCAM: AC-5, DA-1	**Related Controls Requirement(s):** AU-4

ASSESSMENT PROCEDURE: AU-5.1

Assessment Objective

Determine if:
the organization defines designated organizational officials to be alerted in the event of an audit processing failure;

the organization defines in the security plan, explicitly or by reference, personnel to be notified in case of an audit processing failure;

the organization defines additional actions to be taken in the event of an audit processing failure;

the information system takes the additional organization-defined actions in the event of an audit processing failure.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; security plan; information system configuration settings and associated documentation; list of personnel to be notified in case of an audit processing failure; information system audit records; other relevant documents or records.

AU-6 – Audit Review, Analysis, and Reporting (Low)

Control

The organization:
a. Reviews and analyzes information system audit records regularly for indications of inappropriate or unusual activity, and reports findings to designated organizational officials; and
b. Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to CMS operations, CMS assets, individuals, other

organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.

Implementation Standard(s)

1. Review system records for initialization sequences, log-ons and errors; system processes and performance; and system resources utilization to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alert notification for technical personnel review and assessment.
2. Review network traffic, bandwidth utilization rates, alert notifications, and border defense devices to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alerts for technical personnel review and assessment.
3. Investigate suspicious activity or suspected violations on the information system, report findings to appropriate officials and take appropriate action.
4. Use automated utilities to review audit records at least once every fourteen (14) days for unusual, unexpected, or suspicious behavior.
5. Inspect administrator groups on demand but no less than once every thirty (30) days to ensure unauthorized administrator accounts have not been created.

Guidance

Organizations increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to CMS operations, CMS assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

Applicability: All	**Reference(s):** FISCAM: AC-3, AC-4, AC-5, AS-2, DA-1, SM-5; HIPAA: 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(C), 164.312(b); IRS-1075: 5.6.3.3#5.1	**Related Controls Requirement(s):** AU-4, IR-4

ASSESSMENT PROCEDURE: AU-6.1

Assessment Objective

Determine if:
the organization reviews and analyzes information system audit records for indications of inappropriate or unusual activity in accordance with the organization-defined frequency;

the organization adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to CMS operations, CMS assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.

the organization report findings of inappropriate/unusual activities, to designated organizational officials.

the organization meets all the requirements specified in the applicable implementation standard(s).

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit review, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; other relevant documents or records.

ASSESSMENT PROCEDURE: AU-6.2

Assessment Objective

Determine if the organization adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit review, analysis, and reporting; threat information documentation from law enforcement, intelligence community, or other sources; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

AU-6(2) – Enhancement (Low)

Control

[Withdrawn: Incorporated into SI-4].

AU-8 – Time Stamps (Low)

Control

The information system uses internal system clocks to generate time stamps for audit records.

Guidance

Time stamps generated by the information system include both date and time. The time may be expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC.

Applicability: All	**Reference(s):** FISCAM: AC-5	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AU-8.1

Assessment Objective

Determine if the information system uses internal system clocks to generate time stamps for audit records.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing time stamp generation; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

AU-9 – Protection of Audit Information (Low)

Control

The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

Guidance

Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity.

Applicability: All	**Reference(s):** FISCAM: AC-5	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AU-9.1

Assessment Objective

Determine if the information system protects audit information and audit tools from unauthorized:
- access;
- modification;
- deletion.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing protection of audit information; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation, information system audit records; audit tools; other relevant documents or records.

AU-11 – Audit Record Retention (Low)

Control

The organization retains audit records for ninety (90) days and archive old records for one (1) year to provide support for after-the-fact investigations of security incidents and to meet regulatory and CMS information retention requirements.

Guidance

The organization retains audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions. Standard categorizations of audit records relative to such types of actions and standard response processes for each type of action are developed and disseminated. The National Archives and Records Administration (NARA) General Records Schedules (GRS) provide federal policy on record retention.

Applicability: All	**Reference(s):** FISCAM: AC-5	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AU-11.1

Assessment Objective

Determine if:
the retention period for audit records is consistent with the records retention policy;

the organization retains audit records for the organization-defined time period consistent with the records retention policy to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit record retention; security plan; organization-defined retention period for audit records; information system audit records; other relevant documents or records.

AU-12 – Audit Generation (Low)

Control

The information system:
a. Provides audit record generation capability for the following events in addition to those specified in other controls:
- All successful and unsuccessful authorization attempts.
- All changes to logical access control authorities (e.g., rights, permissions).
- All system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services.
- The audit trail shall capture the enabling or disabling of audit report generation services.
- The audit trail shall capture command line changes, batch file changes and queries made to the system (e.g., operating system, application, and database).
b. Allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and
c. Generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.

Guidance

Audits records can be generated from various components within the information system. The list of audited events is the set of events for which audits are to be generated. This set of events is typically a subset of the list of all events for which the system is capable of generating audit records (i.e., auditable events).

Applicability: All	**Reference(s):**	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AU-12.1

Assessment Objective

Determine if:
the organization defines the information system components that provide audit record generation capability for the list of auditable events defined in AU-2;

the information system provides audit record generation capability, at organization-defined information system components, for the list of auditable events defined in AU-2;

the information system allows designated organizational personnel to select which auditable events are to be audited by specific components of the system;

the information system generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing audit record generation; security plan; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.

Security Assessment and Authorization (CA) – *Management*

CA-1 – Security Assessment and Authorization Policies and Procedures (Low)		
Control The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days: a. Formal, documented security assessment and authorization policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security assessment and authorization policies and associated security assessment and authorization controls.		
Guidance This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the security assessment and authorization family [formerly called Certification and Accreditation [C&A] family and process). The policies and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The security assessment/authorization policies can be included as part of the general information security policy for the organization. Security assessment/authorization procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the security assessment and authorization policy.		
Applicability: All	**Reference(s):** FISCAM: AS-1, SM-1, SM-3; HIPAA: 164.308(a)(8); HSPD 7: F(19); IRS-1075: 5.6.1.4#1.1-2	**Related Controls Requirement(s):** CA-6
ASSESSMENT PROCEDURE: CA-1.1		
Assessment Objective Determine if: the organization develops and formally documents security assessment and authorization policy; the organization security assessment and authorization policy addresses: - purpose; - scope; - roles and responsibilities; - management commitment; - coordination among organizational entities; - compliance; the organization disseminates formal documented security assessment and authorization policy to elements within the organization having associated security assessment and authorization roles and responsibilities; the organization develops and formally documents security assessment and authorization procedures; the organization security assessment and authorization procedures facilitate implementation of the security assessment and authorization policy and associated security assessment and authorization controls; the organization disseminates formal documented security assessment and authorization procedures to elements within the organization having associated security assessment and authorization roles and responsibilities; the organization reviews/updates the security assessment and authorization policies and procedures within every three hundred sixty-five (365) days;		
Assessment Methods And Objects **Examine:** Security assessment and authorization policies and procedures; other relevant documents or records.		

CA-2 – Security Assessments (Low)

Control

The organization:
a. Develops a security assessment plan that describes the scope of the assessment including:
- Security controls and control enhancements under assessment;
- Assessment procedures to be used to determine security control effectiveness; and
- Assessment environment, assessment team, and assessment roles and responsibilities;
b. Assesses the security controls in the information system within every three hundred sixty-five (365) days in accordance with the CMS Information Security (IS) Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements (CMSR) Standard, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system;
c. Produces a security assessment report that documents the results of the assessment; and
d. Provides the results of the security control assessment within every three hundred sixty-five (365) days, in writing, to the Business Owner who is responsible for reviewing the assessment documentation and updating system security documentation where necessary to reflect any changes to the system.

Implementation Standard(s)

1. A security assessment of all security controls must be conducted prior to issuing the initial authority to operate for all newly implemented systems.
2. The annual security assessment requirement mandated by OMB requires all CMSRs attributable to a system or application to be assessed over a 3-year period. To meet this requirement, a subset of the CMSRs shall be tested each year so that all security controls are tested during a 3-year period.
3. The Business Owner notifies the CMS CISO within thirty (30) days whenever updates are made to system security authorization artifacts or significant role changes occur (e.g., Business Owner, System Developer/Maintainer, ISSO).

Guidance

The organization assesses the security controls in an information system as part of: (i) security authorization or reauthorization; (ii) meeting the FISMA requirement for annual assessments; (iii) continuous monitoring; and (iv) testing/evaluation of the information system as part of the system development life cycle process. The assessment report documents the assessment results in sufficient detail as deemed necessary by CMS, to determine the accuracy and completeness of the report and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the information system. The FISMA requirement for (at least) annual security control assessments should not be interpreted by organizations as adding additional assessment requirements to those requirements already in place in the security authorization process. To satisfy the FISMA annual assessment requirement, organizations can draw upon the security control assessment results from any of the following sources, including but not limited to: (i) assessments conducted as part of an information system authorization or reauthorization process; (ii) continuous monitoring (see CA-7); or (iii) testing and evaluation of an information system as part of the ongoing system development life cycle (provided that the testing and evaluation results are current and relevant to the determination of security control effectiveness). Existing security control assessment results are reused to the extent that they are still valid and are supplemented with additional assessments as needed.
Subsequent to the initial authorization of the information system and in accordance with OMB policy, the organization assesses a subset of the security controls annually during continuous monitoring. The organization establishes the security control selection criteria and subsequently selects a subset of the security controls within the information system and its environment of operation for assessment. Those security controls that are the most volatile (i.e., controls most affected by ongoing changes to the information system or its environment of operation) or deemed critical to protecting CMS operations and assets, individuals, other organizations, and the Nation are assessed more frequently in accordance with an organizational assessment of risk. All other controls are assessed at least once during the information system's three-year authorization cycle. The organization can use the current year's assessment results from any of the above sources to meet the FISMA annual assessment requirement provided that the results are current, valid, and relevant to determining security control effectiveness. External audits (e.g., audits conducted by external entities such as regulatory agencies) are outside the scope of this control.

Applicability: All	**Reference(s):** FISCAM: AC-6, AS-1, AS-3, SM-5; HIPAA: 164.306(e), 164.308(a)(8); HSPD 7: D(11), F(19); IRS-1075: 5.6.1.4#1.3, 6.3.5#1	**Related Controls Requirement(s):** CA-4, CA-6, CA-7, CA-7(1), CA-7(2), SA-11, SI-2

ASSESSMENT PROCEDURE: CA-2.1

Assessment Objective

Determine if:
the organization develops a security assessment plan for the information system;

the security assessment plan describes the scope of the assessment including:
- security controls and control enhancements under assessment;
- assessment procedures to be used to determine security control effectiveness;
- assessment environment, assessment team, and assessment roles and responsibilities.

the organization meets all the requirements specified in the applicable implementation standard(s).

Assessment Methods And Objects

Examine: Security assessment policy; procedures addressing security assessments; security plan; security assessment plan; assessment evidence; other relevant documents or records.

ASSESSMENT PROCEDURE: CA-2.2

Assessment Objective

Determine if:
the organization assesses the security controls in the information system within every three hundred sixty-five (365) days in accordance with the CMS IS ARS Including CMSR Standard, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system;

the organization provides the results of the security control assessment within every 365 days, in writing, to the Business Owner;

the Business Owner reviews the assessment documentation and updates system security documentation where necessary to reflect any changes to the system;

the results of the security control assessment are provided, in writing, to the authorizing official or authorizing official designated representative.

Assessment Methods And Objects

Examine: Security assessment and authorization policy; procedures addressing security assessments; security plan; security assessment plan; security assessment report; security assessment evidence; plan of action and milestones; other relevant documents or records.

CA-3 – Information System Connections (Low)

Control

The organization:
a. Authorizes connections from the information system to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements;
b. Documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and
c. Monitors the information system connections on an ongoing basis verifying enforcement of security requirements.

Implementation Standard(s)

1. Record each system interconnection in the System Security Plan (SSP) and Information Security (IS) Risk Assessment (RA) for the CMS system that is connected to the remote location.

Guidance

This control applies to dedicated connections between information systems and does not apply to transitory, user-controlled connections such as email and website browsing. The organization carefully considers the risks that may be introduced when information systems are connected to other systems with different security requirements and security controls, both within the organization and external to the organization. Authorizing officials determine the risk associated with each connection and the appropriate controls employed. If the interconnecting systems have the same authorizing official, an Interconnection Security Agreement is not required. Rather, the interface characteristics between the interconnecting information systems are described in the security plans for the respective systems. If the interconnecting systems have different authorizing officials but the authorizing officials are in the same organization, the organization determines whether an Interconnection Security Agreement is required, or alternatively, the interface characteristics between systems are described in the security plans of the respective systems. Instead of developing an Interconnection Security Agreement, organizations may choose to incorporate this information into a formal contract, especially if the interconnection is to be established between CMS and a nonfederal (private sector) organization. In every case, documenting the interface characteristics is required, yet the formality and approval process vary considerably even though all accomplish the same fundamental objective of managing the risk being incurred by the interconnection of the information systems. Risk considerations also include information systems sharing the same networks. Information systems may be identified and authenticated as devices in accordance with IA-3.

Applicability: All	**Reference(s):** FISCAM: AC-1, SM-1; HSPD 7: F(19)	**Related Controls Requirement(s):** SA-9, SC-7

ASSESSMENT PROCEDURE: CA-3.1

Assessment Objective

Determine if:
the organization identifies connections to external information systems (i.e., information systems outside of the authorization boundary);

the organization authorizes connections from the information system to external information systems through the use of Interconnection Security Agreements;

the organization documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated;

the organization monitors the information system connections on an ongoing basis to verify enforcement of security requirements.

the organization meets all the requirements specified in the applicable implementation standard(s).

Assessment Methods And Objects

Examine: Access control policy; procedures addressing information system connections; system and communications protection policy; information system interconnection security agreements; security plan; information system design documentation; security assessment report; plan of action and milestones; other relevant documents or records.

CA-4 – Security Certification (Low)

Control

[Withdrawn: Incorporated into CA-2].

CA-5 – Plan of Action and Milestones (POA&M) (Low)

Control

The organization:
a. Develops and submits a Plan of Action and Milestones (POA&M) for the information system within thirty (30) days of the final results for every internal/external audit/review or test (e.g., ST&E, penetration test) to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and
b. Updates and submits existing POA&M monthly until all the findings are resolved based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

Guidance

The POA&M is a key document in the security authorization package and is subject to federal reporting requirements established by OMB.

Applicability: All	**Reference(s):** FISCAM: AS-1, SM-5, SM-6; HSPD 7: F(19), G(24); IRS-1075: 5.6.1.4#1.4	**Related Controls Requirement(s):** CA-7

ASSESSMENT PROCEDURE: CA-5.1

Assessment Objective

Determine if:
the organization develops a plan of action and milestones for the information system within thirty (30) days of the final results for every internal/external audit/review or test;

the plan of action and milestones documents the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system;

the organization defines in the security plan, explicitly or by reference, the frequency of plan of action and milestone updates;

the organization updates and submits existing POA&M monthly until all the findings are resolved based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

Assessment Methods And Objects

Examine: Security assessment and authorization policy; procedures addressing plan of action and milestones; security plan; security assessment plan; security assessment report; assessment evidence; plan of action and milestones; other relevant documents or records.

CA-5(1) – Enhancement (Low)

Control

The organization employs automated mechanisms to help ensure that the POA&M for the information system is accurate, up to date, and readily available.

Applicability: All	**Reference(s):**	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: CA-5(1).1

Assessment Objective

Determine if the organization employs automated mechanisms to help ensure that the plan of action and milestones for the information system is:
- accurate;
- up to date;
- readily available.

Assessment Methods And Objects

Examine: Security assessment and authorization policy; procedures addressing plan of action and milestones; information system design documentation, information system configuration settings and associated documentation; plan of action and milestones; other relevant documents or records.

CA-6 – Security Authorization (Low)

Control

The organization updates the security authorization:
- At least every three (3) years;
- When substantial changes are made to the system;
- When changes in requirements result in the need to process data of a higher sensitivity;
- When changes occur to authorizing legislation or federal requirements;
- After the occurrence of a serious security violation which raises questions about the validity of an earlier security authorization; and
- Prior to expiration of a previous security authorization.

Guidance

Security authorization is the official management decision, conveyed through the authorization decision document, given by the CMS CIO or his/her designated representative (i.e., authorizing official) to authorize operation of an information system and to explicitly accept the risk to CMS operations and assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls. Explicit authorization to operate the information system is provided by the CMS CIO or his/her designated representative prior to a system being placed into operations.

Through the security authorization process, the CMS CIO is accountable for the security risks associated with CMS information system operations. Through the employment of a comprehensive continuous monitoring process, the critical information contained in the authorization package (i.e., the security plan (including risk assessment), the security assessment report, and the plan of action and milestones) is updated on an ongoing basis, providing the CMS CIO and the applicable information system Business Owner with an up-to-date status of the security state of the information system.

To reduce the administrative cost of security reauthorization, the CMS CIO uses the results of the continuous monitoring process to the maximum extent possible as the basis for rendering a reauthorization decision. OMB policy requires that federal information systems are reauthorized at least every three years or when there is a significant change to the system.

A significant change to the information system includes a physical, administrative, or technical modification that alters the degree of protection required. Examples include, but are not limited to, changes in operating systems, computer hardware, firmware, operational environment, or system boundaries; new services or applications; or other conditions that potentially impact the system's security posture or authorization status.

Applicability: All	**Reference(s):** FISCAM: SM-2, SM-5; HSPD 7: F(19)	**Related Controls Requirement(s):** CA-1, CA-2, CA-4, CA-7

ASSESSMENT PROCEDURE: CA-6.1

Assessment Objective

Determine if:
the organization defines in the security plan, explicitly or by reference, the frequency of authorization updates, not to exceed three years;

the organization updates the security authorization:
- at least every three (3) years;
- when substantial changes are made to the system;
- when changes in requirements result in the need to process data of a higher sensitivity;
- when changes occur to authorizing legislation or federal requirements;
- after the occurrence of a serious security violation which raises questions about the validity of an earlier security authorization; and
- prior to expiration of a previous security authorization;

a senior organizational official signs and approves the security authorization package.

Assessment Methods And Objects

Examine: Security assessment and authorization policy; procedures addressing security authorization; security authorization package (including security plan; security assessment report; plan of action and milestones; authorization statement); other relevant documents or records.

CA-7 – Continuous Monitoring (Low)

Control

The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes:
a. A configuration management process for the information system and its constituent components;
b. A determination of the security impact of changes to the information system and environment of operation;
c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; and
d. Reporting the security state of the information system to appropriate organizational officials within every three hundred sixty-five (365) days.

Guidance

A continuous monitoring program allows an organization to maintain the security authorization of an information system over time in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and missions/business processes. Continuous monitoring of security controls using automated support tools facilitates near real-time risk management and promotes organizational situational awareness with regard to the security state of the information system. The implementation of a continuous monitoring program results in ongoing updates to the security plan, the security assessment report, and the plan of action and milestones, the three principal documents in the security authorization package. A rigorous and well executed continuous monitoring program significantly reduces the level of effort required for the reauthorization of the information system. Continuous monitoring activities are scaled in accordance with the security categorization of the information system.

Applicability: All	**Reference(s):** FISCAM: AS-1, SM-5; HSPD 7: F(19)	**Related Controls Requirement(s):** CA-2, CA-4, CA-5, CA-6, CM-4, SI-2

ASSESSMENT PROCEDURE: CA-7.1

Assessment Objective

Determine if:
the organization establishes a continuous monitoring strategy and program;

the organization defines the frequency for reporting the security state of the information system to appropriate organizational officials;

the organization defines organizational officials to whom the security state of the information system should be reported;

the organization implements a continuous monitoring program that includes:
- a configuration management process for the information system and its constituent components;
- a determination of the security impact of changes to the information system and environment of operation;
- ongoing security control assessments in accordance with the organizational continuous monitoring strategy;

- reporting the security state of the information system to appropriate organizational officials in accordance with organization-defined frequency.

Assessment Methods And Objects

Examine: Security assessment and authorization policy; procedures addressing continuous monitoring of information system security controls; procedures addressing configuration management; security plan; security assessment report; plan of action and milestones; information system monitoring records; configuration management records, security impact analyses; status reports; other relevant documents or records.

CA-7(1) – Enhancement (Low)

Control

The use of independent security assessment agents or teams to monitor security controls is not required. However, if the organization employs an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis, this can be used to satisfy ST&E requirements.

Guidance

The organization can extend and maximize the value of the ongoing assessment of security controls during the continuous monitoring process by requiring an independent assessor or team to assess all of the security controls during the information system's three-year authorization cycle. See supplemental guidance for CA-2, enhancement (1), for further information on assessor independence.

Applicability: All	**Reference(s):**	**Related Controls Requirement(s):** AC-9, CA-2

ASSESSMENT PROCEDURE: CA-7(1).1

Assessment Objective

Determine if the organization employs an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis.

Assessment Methods And Objects

Examine: Security assessment and authorization policy; procedures addressing continuous monitoring of information system security controls; security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records.

CA-7(2) – Enhancement (Low)

Control

CMS plans, schedules, and conducts automated or manual assessments on a continuous and unannounced basis, of all CMS information systems and information systems that are processing data on behalf of or directly for CMS including, but not limited to, in-depth monitoring of systems and networks, vulnerability and configuration scanning, and announced penetration testing to ensure compliance with all vulnerability mitigation procedures.

Guidance

Examples of vulnerability mitigation procedures are contained in Information Assurance Vulnerability Alerts. Testing is intended to ensure that the information system continues to provide adequate security against constantly evolving threats and vulnerabilities. Conformance testing could also provide evidence of independent validation. See supplemental guidance for CA-2, enhancement (2) for further information on malicious user testing, penetration testing, and other forms of security testing.

Applicability: All	**Reference(s):**	**Related Controls Requirement(s):** CA-2

ASSESSMENT PROCEDURE: CA-7(2).1

Assessment Objective

Determine if:
the organization defines:
- the forms of security testing to be included in planning, scheduling, and security control assessments selecting from in-depth monitoring, malicious user testing, penetration testing, or an organization-defined form of security testing to ensure compliance with all vulnerability mitigation procedures;
- the frequency for conducting each form of security testing;

- whether the security testing will be announced or unannounced;

the organization plans, schedules, and conducts assessments using organization-defined forms of security testing in accordance with the organization-defined frequency and assessment techniques established for each form of testing to ensure compliance with all vulnerability mitigation procedures.

Assessment Methods And Objects

Examine: Security assessment and authorization policy; procedures addressing continuous monitoring of information system security controls; procedures addressing vulnerability mitigation; security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records.

Interview: Organizational personnel with continuous monitoring responsibilities.

Configuration Management (CM) – *Operational*

CM-1 – Configuration Management Policy and Procedures (Low)

Control

The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:
a. A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

Guidance

This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the configuration management family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The configuration management policy can be included as part of the general information security policy for the organization. Configuration management procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the configuration management policy.

Applicability: All	**Reference(s):** FISCAM: AS-1, CM-1, CP-2, SM-1, SM-3; IRS-1075: 5.6.2.3#1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: CM-1.1

Assessment Objective

Determine if:
the organization develops and formally documents configuration management policy;

the organization configuration management policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented configuration management policy to elements within the organization having associated configuration management roles and responsibilities;

the organization develops and formally documents configuration management procedures;

the organization configuration management procedures facilitate implementation of the configuration management policy and associated configuration management controls;

the organization disseminates formal documented configuration management procedures to elements within the organization having associated configuration management roles and responsibilities;

the organization reviews/updates the configuration management policy and procedures within every three hundred sixty-five (365) days.

Assessment Methods And Objects

Examine: Configuration management policy and procedures; other relevant documents or records.

CM-2 – Baseline Configuration (Low)

Control

The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

Guidance

This control establishes a baseline configuration for the information system and its constituent components including communications and connectivity-related aspects of the system. The baseline configuration provides information about the components of a CMS information system (e.g., the standard software load for a workstation, server, network component, or mobile device including operating system/installed applications with current version numbers and patch information), network topology, and the logical placement of the component within the system architecture. The baseline configuration is a documented, up-to-date specification to which the information system is built. Maintaining the baseline configuration involves creating new baselines as the information system changes over time. The baseline configuration of the information system is consistent with CMS' enterprise architecture.

Applicability: All	**Reference(s):**	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: CM-2.1

Assessment Objective

Determine if:
the organization develops and documents a baseline configuration of the information system;

the organization maintains, under configuration control, a current baseline configuration of the information system.

the organization documents deviations from the baseline configuration, in support of mission needs/objectives.

Assessment Methods And Objects

Examine: Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; enterprise architecture documentation; information system design documentation; information system architecture and configuration documentation; other relevant documents or records.

CM-4 – Security Impact Analysis (Low)

Control

The organization analyzes changes to the information system to determine potential security impacts prior to change implementation. Activities associated with configuration changes to the information system are audited.

Guidance

Security impact analyses are conducted by organizational personnel with information security responsibilities, including for example, Information System Administrators, Information System Security Officers, Information System Security Managers, and Information System Security Engineers. Individuals conducting security impact analyses have the appropriate skills and technical expertise to analyze the changes to information systems and the associated security ramifications. Security impact analysis may include, for example, reviewing information system documentation such as the security plan to understand how specific security controls are implemented within the system and how the changes might affect the controls. Security impact analysis may also include an assessment of risk to understand the impact of the changes and to determine if additional security controls are required. Security impact analysis is scaled in accordance with the security categorization of the information system.

Applicability: All	**Reference(s):** FISCAM: AS-3, CM-3, CM-4, SM-5	**Related Controls Requirement(s):** CA-7, CM-3

ASSESSMENT PROCEDURE: CM-4.1

Assessment Objective

Determine if the organization analyzes changes to the information system to determine potential security impacts prior to change implementation.

Assessment Methods And Objects

Examine: Configuration management policy; configuration management plan; procedures addressing security impact analysis for changes to the information system; security impact analysis documentation; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records.

CM-6 – Configuration Settings (Low)

Control

The organization:
a. Establishes and documents mandatory configuration settings for information technology products employed within the information system using the latest security configuration guidelines listed in Implementation Standard 1 that reflect the most restrictive mode consistent with operational requirements;
b. Implements the configuration settings;
c. Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and
d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

Implementation Standard(s)

1. Security configuration guidelines may be developed by different federal agencies, so it is possible that a guideline could include configuration information that conflicts with another agency or CMS guideline. To resolve configuration conflicts among multiple security guidelines, the CMS hierarchy for implementing all security configuration guidelines is as follows:
(a) CMS
(b) DHHS
(c) OMB
(d) NIST
(e) DISA.

Guidance

Configuration settings are the configurable security-related parameters of information technology products that are part of the information system. Security-related parameters are those parameters impacting the security state of the system including parameters related to meeting other security control requirements. Security-related parameters include, for example, registry settings; account, file, and directory settings (i.e., permissions); and settings for services, ports, protocols, and remote connections. Organizations establish organization-wide mandatory configuration settings from which the settings for a given information system are derived. A security configuration checklist (sometimes referred to as a lockdown guide, hardening guide, security guide, security technical implementation guide [STIG], or benchmark) is a series of instructions or procedures for configuring an information system component to meet operational requirements. Checklists can be developed by information technology developers and vendors, consortia, academia, industry, federal agencies (and other government organizations), and others in the public and private sectors. An example of a security configuration checklist is the Federal Desktop Core Configuration (FDCC) which potentially affects the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content Automation Protocol (SCAP) and defined standards within the protocol (e.g., Common Configuration Enumeration) provide an effective method to uniquely identify, track, and control configuration settings. OMB establishes federal policy on configuration requirements for federal information systems.

Applicability: All	**Reference(s):** FISCAM: AC-3, AS-3, CM-2, CM-3; IRS-1075: 5.6.2.3#1	**Related Controls Requirement(s):** CM-3, CM-8, SI-4

ASSESSMENT PROCEDURE: CM-6.1

Assessment Objective

Determine if:
the organization defines security configuration checklists to be used to establish and document mandatory configuration settings for the information system technology products employed;

the organization-defined security configuration checklists reflect the most restrictive mode consistent with operational requirements;

the organization establishes and documents mandatory configuration settings for information technology products employed within the information system using organization-defined security configuration checklists;

the organization implements the security configuration settings;

the organization identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements;

the organization monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

the organization meets all the requirements specified in the applicable implementation standard(s).

Assessment Methods And Objects

Examine: Configuration management policy; configuration management plan; procedures addressing configuration settings for the information system; security plan; information system configuration settings and associated documentation; security configuration checklists; other relevant documents or records.

CM-7 – Least Functionality (Low)

Control

The organization configures the information system to provide only essential capabilities and specifically disables, prohibits, or restricts the use of system services, ports, network protocols, and capabilities that are not explicitly required for system or application functionality. A list of specifically needed system services, ports, and network protocols will be maintained and documented in the SSP; all others will be disabled.

Guidance

Information systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential CMS operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from a single component of an information system, but doing so increases risk over limiting the services provided by any one component. Where feasible, organizations limit component functionality to a single function per device (e.g., email server or web server, not both). The functions and services provided by CMS information systems, or individual components of CMS information systems, are carefully reviewed to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, auto-execute, file sharing). Organizations consider disabling unused or unnecessary physical and logical ports and protocols (e.g., Universal Serial Bus [USB], File Transfer Protocol [FTP], Internet Protocol Version 6 [IPv6], Hyper Text Transfer Protocol [HTTP]) on information system components to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling. Organizations can utilize network scanning tools, intrusion detection and prevention systems, and end-point protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services.

Applicability: All	**Reference(s):** FISCAM: AC-3, CM-3; IRS-1075: 5.6.2.3#1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: CM-7.1

Assessment Objective

Determine if:
the organization defines for the information system prohibited or restricted:
- functions;
- ports;
- protocols;
- services;

the organization configures the information system to provide only essential capabilities;

the organization configures the information system to specifically prohibit or restrict the use of organization-defined:
- functions;
- ports;
- protocols; and/or
- services.

Assessment Methods And Objects

Examine: Configuration management policy; configuration management plan; procedures addressing least functionality in the information system; security plan; information system configuration settings and associated documentation; security configuration checklists; other relevant documents or records.

CM-8 – Information System Component Inventory (Low)

Control

The organization develops, documents, and maintains an inventory of information system components that:
a. Accurately reflects the current information system;

b. Is consistent with the authorization boundary of the information system;
c. Is at the level of granularity deemed necessary for tracking and reporting;
d. Includes manufacturer, model/type, serial number, version number, location (i.e., physical location and logical position within the information system architecture), and ownership; and
e. Is available for review and audit by designated organizational officials.

Guidance

Information deemed to be necessary by the organization to achieve effective property accountability can include, for example, hardware inventory specifications (manufacturer, type, model, serial number, physical location), software license information, information system/component owner, and for a networked component/device, the machine name and network address.

Applicability: All	**Reference(s):** FISCAM: CM-2, SM-1; HIPAA: 164.310(d)(1), 164.310(d)(2)(iii)	**Related Controls Requirement(s):** CM-6

ASSESSMENT PROCEDURE: CM-8.1

Assessment Objective

Determine if:
the organization defines information deemed necessary to achieve effective property accountability;

the organization develops, documents, and maintains an inventory of information system components that:
- accurately reflects the current information system;
- is consistent with the authorization boundary of the information system;
- is at the level of granularity deemed necessary for tracking and reporting;
- includes organization-defined information deemed necessary to achieve effective property accountability;
- is available for review and audit by designated organizational officials.

Assessment Methods And Objects

Examine: Configuration management policy; configuration management plan; procedures addressing information system component inventory; security plan; information system inventory records; other relevant documents or records.

Contingency Planning (CP) – *Operational*

CP-1 – Contingency Planning Policy and Procedures (Low)

Control

The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:
a. A formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.

Guidance

This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the contingency planning family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The contingency planning policy can be included as part of the general information security policy for the organization. Contingency planning procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the contingency planning policy.

Applicability: All	**Reference(s):** FISCAM: AS-1, AS-5, CP-1, CP-3, SM-1, SM-3; HIPAA: 164.308(a)(7)(i), 164.308(a)(7)(ii)(B); IRS-1075: 5.6.2.2#1.1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: CP-1.1

Assessment Objective

Determine if:
the organization develops and formally documents contingency planning policy;

the organization contingency planning policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented contingency planning policy to elements within the organization having associated contingency planning roles and responsibilities;

the organization develops and formally documents contingency planning procedures;

the organization contingency planning procedures facilitate implementation of the contingency planning policy and associated contingency planning controls;

the organization disseminates formal documented contingency planning procedures to elements within the organization having associated contingency planning roles and responsibilities;

the organization reviews/updates the contingency planning policy and procedures within every three hundred sixty-five (365) days.

Assessment Methods And Objects

Examine: Contingency planning policy and procedures; other relevant documents or records.

CP-2 – Contingency Plan (Low)

Control

The organization:
a. Develops a Contingency Plan (CP) for the information system that:
- Identifies essential CMS missions and business functions and associated contingency requirements;

- Provides recovery objectives, restoration priorities, and metrics;
- Addresses contingency roles, responsibilities, assigned individuals with contact information;
- Addresses maintaining essential CMS missions and business functions despite an information system disruption, compromise, or failure;
- Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and
- Is reviewed and approved by designated officials within the organization;
b. Distributes copies of the CP plan to key contingency personnel (identified by name and/or by role) and organizational elements;
c. Coordinates contingency planning activities with incident handling activities;
d. Reviews the CP for the information system within every three hundred sixty-five (365) days;
e. Revises the CP to address changes to the organization, information system, or environment of operation and problems encountered during CP implementation, execution, or testing; and
f. Communicates CP changes to key contingency personnel (identified by name and/or by role) and organizational elements.

Guidance

Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for CMS mission/business operations. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. Information system recovery objectives are consistent with applicable laws, Executive Orders, directives, policies, standards, or regulations. In addition to information system availability, contingency plans also address other security-related events resulting in a reduction in mission/business effectiveness, such as malicious attacks compromising the confidentiality or integrity of the information system. Examples of actions to call out in contingency plans include, for example, graceful degradation, information system shutdown, fall back to a manual mode, alternate information flows, or operating in a mode that is reserved solely for when the system is under attack. Copies of the current CP are stored in a secure location at an alternate site accessible by management and other key personnel.

Applicability: All	**Reference(s):** FISCAM: AS-5, CP-1, CP-2, CP-3; HIPAA: 164.308(a)(7)(ii)(E), 164.312(a)(2)(ii); HSPD 7: G(22)(i); IRS-1075: 5.6.2.2#1.3	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: CP-2.1

Assessment Objective

Determine if:
the organization develops a contingency plan for the information system that:
- identifies essential missions and business functions and associated contingency requirements;
- provides recovery objectives, restoration priorities, and metrics;
- addresses contingency roles, responsibilities, assigned individuals with contact information;
- addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
- addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented;
-is reviewed and approved by designated officials within the organization;

the organization defines key contingency personnel (identified by name and/or by role) and organizational elements designated to receive copies of the contingency plan;

the organization distributes copies of the contingency plan to organization-defined key contingency personnel and organizational elements.

Assessment Methods And Objects

Examine: Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; security plan; other relevant documents or records.

ASSESSMENT PROCEDURE: CP-2.2

Assessment Objective

Determine if:
the organization coordinates contingency planning activities with incident handling activities;

the organization defines the frequency of contingency plan reviews;

the organization reviews the contingency plan for the information system in accordance with the organization-defined frequency;

the organization revises the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution or testing;

the organization communicates contingency plan changes to the key contingency personnel and organizational elements.

Assessment Methods And Objects

Examine: Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; security plan; other relevant documents or records.

CP-3 – Contingency Training (Low)

Control

The organization trains operational and support personnel (including managers and users of the information system) in their contingency roles and responsibilities with respect to the information system and provides refresher training within every three hundred sixty-five (365) days.

Guidance

Managers, responsible for contingency operations, and technical personnel should meet, at a minimum, once a year for review of contingency policies and procedures. Each review session should be documented and confirmed that appropriate training has been completed.

Applicability: All	**Reference(s):** FISCAM: CP-2; HSPD 7: G(22)(i)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: CP-3.1

Assessment Objective

Determine if:
the organization provides initial contingency training to personnel with contingency roles and responsibilities with respect to the information system;

the organization defines in the security plan, explicitly or by reference, the frequency of refresher contingency training and the frequency is at least annually;

the organization provides refresher training in accordance with organization-defined frequency.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing contingency training; contingency training curriculum; contingency training material; security plan; contingency training records; other relevant documents or records.

CP-4 – Contingency Plan Testing and Exercises (Low)

Control

The organization:
a. Tests and/or exercises the contingency plan for the CMS information system within every three hundred sixty-five (365) days using defined tests and exercises, such as the tabletop test in accordance with the current CMS contingency plan procedure to determine the plan's effectiveness and the organization's readiness to execute the plan; and
b. Documents and reviews the contingency plan test/exercise results and initiates reasonable and appropriate corrective actions to close or reduce the impact of contingency plan failures and deficiencies.

Guidance

There are several methods for testing and/or exercising contingency plans to identify potential weaknesses (e.g., checklist, walk-through/tabletop, simulation: parallel, full interrupt). Contingency plan testing and/or exercises include a determination of the effects on CMS operations and assets (e.g., reduction in mission capability) and individuals arising due to contingency operations in accordance with the plan.

Applicability: All	**Reference(s):** FISCAM: AS-5, CP-2, CP-4; HIPAA: 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(D); HSPD 7: G(22)(i); IRS-1075: 5.6.2.2#1.2	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: CP-4.1

Assessment Objective

Determine if:
the organization defines in the security plan, explicitly or by reference, the contingency plan tests and/or exercises to be conducted;

the organization defines in the security plan, explicitly or by reference, the frequency of contingency plan tests and/or exercises and the frequency is at least annually;

the organization tests/exercises the contingency plan using organization-defined tests/exercises in accordance with organization-defined frequency;

the organization reviews the contingency plan test/exercise results and takes corrective actions.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan, procedures addressing contingency plan testing and exercises; security plan; contingency plan testing and/or exercise documentation; other relevant documents or records.

CP-5 – Contingency Plan Update (Low)

Control

[Withdrawn: Incorporated into CP-2].

CP-9 – Information System Backup (Low)

Control

The organization:
a. Conducts backups of user-level information contained in the CMS information system in accordance with the frequency specified in Implementation Standard 1;
b. Conducts backups of system-level information contained in the CMS information system in accordance with the frequency specified in Implementation Standard 1;
c. Conducts backups of CMS information system documentation including security-related documentation and other forms of data, including paper records; and
d. Protects the confidentiality and integrity of CMS backup information at the storage location.

Implementation Standard(s)

1. Perform backups of user-level and system-level information (including system state information) every month.

Guidance

System-level information includes, for example, system-state information, operating system and application software, and licenses. Digital signatures and cryptographic hashes are examples of mechanisms that can be employed by organizations to protect the integrity of information system backups. An organizational assessment of risk guides the use of encryption for protecting backup information. The protection of system backup information while in transit is beyond the scope of this control.
The transfer rate of backup information to an alternate storage site (if so designated) is guided by the CMS recovery time objectives and recovery point objectives. Checkpoint capabilities are part of any backup operation that updates files and consumes large amounts of information system time.

Applicability: All	**Reference(s):** FISCAM: AS-5, CP-2; HIPAA: 164.308(a)(7)(ii)(A), 164.312(c)(1); IRS-1075: 5.6.2.2#1.6	**Related Controls Requirement(s):** MP-4, MP-5

ASSESSMENT PROCEDURE: CP-9.1

Assessment Objective

Determine if:
the organization backs up user-level information in accordance with the frequency specified in Implementation Standard 1;

the organization backs up system-level information in accordance with the frequency specified in Implementation Standard 1;

the organization backs up information system documentation (including security-related information and other forms of data).

the organization meets all the requirements specified in the applicable implementation standard(s).

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; security plan; backup storage location(s); information system backup logs or records; other relevant documents or records.

ASSESSMENT PROCEDURE: CP-9.2

Assessment Objective

Determine if the organization protects the confidentiality and integrity of backup information at the storage location.

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; information system design documentation; information system configuration settings and associated documentation; backup storage location(s); other relevant documents or records.

CP-9(4) – Enhancement (Low)

Control

[Withdrawn: Incorporated into CP-9].

CP-10 – Information System Recovery and Reconstitution (Low)

Control

The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure. Recovery of the information system after a failure or other contingency shall be done in a trusted, secure, and verifiable manner.

Implementation Standard(s)

1. Secure information system recovery and reconstitution includes, but not limited to:
(a) Reset all system parameters (either default or organization-established),
(b) Reinstall patches,
(c) Reestablish configuration settings,
(d) Reinstall application and system software, and
(e) Fully test the system.

Guidance

Recovery is executing information system contingency plan activities to restore essential CMS missions and business functions. Reconstitution takes place following recovery and includes activities for returning the information system to its original functional state before contingency plan activation. Recovery and reconstitution procedures are based on CMS priorities, established recovery point/time and reconstitution objectives, and appropriate metrics. Reconstitution includes the deactivation of any interim information system capability that may have been needed during recovery operations. Reconstitution also includes an assessment of the fully restored information system capability, a potential system reauthorization and the necessary activities to prepare the system against another disruption, compromise, or failure. Recovery and reconstitution capabilities employed by the organization can be a combination of automated mechanisms and manual procedures.

Applicability: All	**Reference(s):** FISCAM: CP-2, CP-3, CP-4; HIPAA: 164.308(a)(7)(ii)(C); HSPD 7: G(22)(i)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: CP-10.1

Assessment Objective

Determine if:
the organization provides automated mechanisms and/or manual procedures for the recovery and reconstitution of the information system to known state after a disruption, compromise, or failure;

the organization provides for the recovery of the information system after a failure or other contingency in a trusted, secure, and verifiable manner.

the organization meets all the requirements specified in the applicable implementation standard(s).

Assessment Methods And Objects

Examine: Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; information system configuration settings and associated documentation; information system design documentation; other relevant documents or records.

CP-10(1) – Enhancement (Low)

Control

[Withdrawn: Incorporated into CP-4].

Identification and Authentication (IA) – *Technical*

IA-1 – Identification and Authentication Policy and Procedures (Low)

Control

The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:
a. A formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

Guidance

This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the identification and authentication family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The identification and authentication policy can be included as part of the general information security policy for the organization. Identification and authentication procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the identification and authentication policy.

Applicability: All	**Reference(s):** FISCAM: AS-1, SM-1, SM-3; IRS-1075: 5.6.3.1#1.1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: IA-1.1

Assessment Objective

Determine if:
the organization develops and formally documents identification and authentication policy;

the organization identification and authentication policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented identification and authentication policy to elements within the organization having associated identification and authentication roles and responsibilities;

the organization develops and formally documents identification and authentication procedures;

the organization identification and authentication procedures facilitate implementation of the identification and authentication policy and associated identification and authentication controls;

the organization disseminates formal documented identification and authentication procedures to elements within the organization having associated identification and authentication roles and responsibilities;

the organization reviews/updates the identification and authentication policy and procedures within every three hundred sixty-five (365) days.

Assessment Methods And Objects

Examine: Identification and authentication policy and procedures; other relevant documents or records.

IA-2 – Identification and Authentication (Organizational Users) (Low)

Control

The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

Implementation Standard(s)

1. Require the use of system and/or network authenticators and unique user identifiers.
2. Help desk support requires user identification for any transaction that has information security implications.

Guidance

Organizational users (i.e., CMS information system users) include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors, guest researchers, individuals from allied nations). Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in AC-14. Unique identification of individuals in group accounts (e.g., shared privilege accounts) may need to be considered for detailed accountability of activity. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof. Access to CMS information systems is defined as either local or network.
Local access is any access to a CMS information system by a user (or process acting on behalf of a user) where such access is obtained by direct connection without the use of a network. Network access is any access to a CMS information system by a user (or process acting on behalf of a user) where such access is obtained through a network connection. Remote access is a type of network access which involves communication through an external network (e.g., the Internet). Internal networks include local area networks, wide area networks, and virtual private networks that are under the control of the organization. For a virtual private network (VPN), the VPN is considered an internal network if the organization establishes the VPN connection between organization-controlled endpoints in a manner that does not require the organization to depend on any external networks across which the VPN transits to protect the confidentiality and integrity of information transmitted. Identification and authentication requirements for information system access by other than organizational users are described in IA-8.
The identification and authentication requirements in this control are satisfied by complying with Homeland Security Presidential Directive 12 consistent with organization-specific implementation plans provided to OMB. In addition to identifying and authenticating users at the information-system level (i.e., at logon), identification and authentication mechanisms are employed at the application level, when necessary, to provide increased information security for the organization.

Applicability: All	**Reference(s):** FISCAM: AC-2, AS-2; HIPAA: 164.312(a)(2)(i), 164.312(d); IRS-1075: 5.6.3.1#1.2, 5.6.3.3#2.3	**Related Controls Requirement(s):** AC-14, AC-17, MA-4

ASSESSMENT PROCEDURE: IA-2.1

Assessment Objective

Determine if:
the information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

the organization meets all the requirements specified in the applicable implementation standard(s).

Assessment Methods And Objects

Examine: Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; list of information system accounts; other relevant documents or records.

IA-2(1) – Enhancement (Low)

Control

The information system uses multifactor authentication for network access to privileged accounts.

Applicability: All	**Reference(s):**	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: IA-2(1).1

Assessment Objective

Determine if:
the organization defines in the security plan, explicitly or by reference, the authentication level for the information system;

the information system uses multifactor authentication for network access to privileged accounts.

Assessment Methods And Objects

Examine: Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; list of privileged information system accounts; other relevant documents or records.

IA-4 – Identifier Management (Low)

Control

The organization manages CMS information system identifiers for users and devices by:
a. Receiving authorization from a designated organizational official to assign a user or device identifier;
b. Selecting an identifier that uniquely identifies an individual or device;
c. Assigning the user identifier to the intended party or the device identifier to the intended device;
d. Preventing reuse of user or device identifiers until all previous access authorizations are removed from the system, including all file accesses for that identifier but not before a period of at least three hundred sixty-five (365) days has expired; and
e. Disabling the user identifier after the time period of inactivity specified in Implementation Standard 1 and deleting disabled accounts during the annual re-certification process.

Implementation Standard(s)

1. Disable user identifiers after three hundred sixty-five (365) days of inactivity.

Guidance

Common device identifiers include media access control (MAC) or Internet protocol (IP) addresses, or device-unique token identifiers. Management of user identifiers is not applicable to shared information system accounts (e.g., guest and anonymous accounts). It is commonly the case that a user identifier is the name of an information system account associated with an individual. In such instances, identifier management is largely addressed by the account management activities of AC-2. IA-4 also covers user identifiers not necessarily associated with an information system account (e.g., the identifier used in a physical security control database accessed by a badge reader system for access to the information system).
Reviews and validation of system users' accounts are conducted to ensure the continued need for access to a system. Identifier management is applicable to shared information system accounts (i.e., guest and anonymous).

Applicability: All	**Reference(s):** FISCAM: AC-2, AC-3, AC-4, AS-2; IRS-1075: 5.6.3.1#2	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: IA-4.1

Assessment Objective

Determine if:
the organization manages information system identifiers for users and devices by:
- receiving authorization from a designated organizational official to assign a user or device identifier;
- selecting an identifier that uniquely identifies an individual or device;
- assigning the user identifier to the intended party or the device identifier to the intended device;
- preventing reuse of user or device identifiers for the organization-defined time period;
- disabling the user identifier after the organization-defined time period of inactivity;

the organization defines in the security plan, explicitly or by reference, the time period of inactivity after which a user identifier is to be disabled.

the organization meets all the requirements specified in the applicable implementation standard(s).

Assessment Methods And Objects

Examine: Identification and authentication policy; procedures addressing identifier management; procedures addressing account management; security plan; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; list of identifiers generated from physical access control devices; other relevant documents or records.

IA-5 – Authenticator Management (Low)

Control

The organization manages CMS information system authenticators for users and devices by:
a. Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator;
b. Establishing initial authenticator content for authenticators defined by the organization;
c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;

d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
e. Changing default content of authenticators upon information system installation;
f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate);
g. Changing/refreshing password authenticators as defined in IA-5(1);
h. Protecting authenticator content from unauthorized disclosure and modification; and
i. Requiring users to take, and having devices implement, specific measures to safeguard authenticators.

Guidance

User authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). Many information system components are shipped with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, present a significant security risk, and therefore, are changed upon installation. The requirement to protect user authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of users and by controls AC-3, AC-6, and SC-28 for authenticators stored within the information system (e.g., passwords stored in a hashed or encrypted format, files containing encrypted or hashed passwords accessible only with super user privileges). The CMS information system supports user authenticator management by security settings and restrictions for various authenticator characteristics including, for example, minimum password length, password composition, validation time window for time synchronous one time tokens, and number of allowed rejections during verification stage of biometric authentication. Measures to safeguard user authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include, for example, certificates and passwords.

Applicability: All	**Reference(s):** FISCAM: AC-2, AS-2; IRS-1075: 5.6.3.1#2	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: IA-5.1

Assessment Objective

Determine if:
the organization defines the time period (by authenticator type) for changing/refreshing authenticators;

the organization manages information system authenticators for users and devices by:
- verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator;
- establishing initial authenticator content for authenticators defined by the organization;
- ensuring that authenticators have sufficient strength of mechanism for their intended use;
- establishing and implementing administrative procedures for initial authenticator distribution;
- establishing and implementing administrative procedures for lost/compromised or damaged authenticators;
- establishing and implementing administrative procedures for revoking authenticators;
- changing default content of authenticators upon information system installation;
- establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if deemed to be appropriate by the organization);
- changing/refreshing authenticators in accordance with the organization-defined time period by authenticator type;
- protecting authenticator content from unauthorized disclosure and modification;
- requiring users to take, and having devices implement, specific measures to safeguard authenticators.

Assessment Methods And Objects

Examine: Identification and authentication policy; procedures addressing authenticator management; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records.

IA-5(1) – Enhancement (Low)

Control

The CMS information system, for password-based authentication:
(a) Automatically forces users (including administrators) to change user account passwords every sixty (60) days and system account passwords every one hundred eighty (180) days;
(b) Prohibits the use of dictionary names or words;

(c) Enforces minimum password complexity consisting of at least eight (8) alphanumeric (i.e., upper- and lower-case letters, and numbers) and/or special characters;
(d) Enforces at least a minimum of four (4) changed characters when new passwords are created;
(e) Encrypts passwords in storage and in transmission;
(f) Enforces password minimum and maximum lifetime restrictions of one (1) day for the minimum, and sixty (60) days for a user account and one hundred eighty (180) days for a system account maximum; and
(g) Prohibits password reuse for one (1) generation prior to reuse.

Guidance

This control enhancement is intended primarily for environments where passwords are used as a single factor to authenticate users, or in a similar manner along with one or more additional authenticators. The enhancement generally does not apply to situations where passwords are used to unlock hardware authenticators. The implementation of such password mechanisms may not meet all of the requirements in the enhancement.

Applicability: All	**Reference(s):**	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: IA-5(1).1

Assessment Objective

Determine if the information system, for password-based authentication:
- enforces the minimum password complexity standards that meet the organization-defined requirements;
- enforces the organization-defined minimum number of characters that must be changed when new passwords are created;
- encrypts passwords in storage and in transmission;
- enforces the organization-defined restrictions for password minimum lifetime and password maximum lifetime parameters;
- prohibits password reuse for the organization-defined number of generations.

Assessment Methods And Objects

Examine: Identification and authentication policy; password policy; procedures addressing authenticator management; security plan; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

IA-6 – Authenticator Feedback (Low)

Control

The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Guidance

The feedback from the information system does not provide information that would allow an unauthorized user to compromise the authentication mechanism. Displaying asterisks when a user types in a password, is an example of obscuring feedback of authentication information.

Applicability: All	**Reference(s):** FISCAM: AC-2; IRS-1075: 5.6.3.1#1.2	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: IA-6.1

Assessment Objective

Determine if the information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Assessment Methods And Objects

Examine: Identification and authentication policy; procedures addressing authenticator feedback; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

IA-7 – Cryptographic Module Authentication (Low)		
Control The information system uses mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.		
Applicability: All	**Reference(s):** FISCAM: AC-4	**Related Controls Requirement(s):**
ASSESSMENT PROCEDURE: IA-7.1		
Assessment Objective Determine if the information system uses mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication. **Assessment Methods And Objects** **Examine:** Identification and authentication policy; procedures addressing cryptographic module authentication; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.		
IA-8 – Identification and Authentication (Non-Organizational Users) (Low)		
Control The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).		
Guidance Non-organizational users include all CMS information system users other than organizational users explicitly covered by IA-2. Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in accordance with AC-14. In accordance with the E-Authentication E-Government initiative, authentication of non-organizational users accessing federal information systems may be required to protect federal, proprietary, or privacy-related information (with exceptions noted for national security systems). Accordingly, a risk assessment is used in determining the authentication needs of the organization. Scalability, practicality, and security are simultaneously considered in balancing the need to ensure ease of use for access to federal information and information systems with the need to protect and adequately mitigate risk to CMS operations, CMS assets, individuals, other organizations, and the Nation. Identification and authentication requirements for CMS information system access by organizational users are described in IA-2. If E-Authentication is used, refer to ARS Appendix D: E-authentication Standard.		
Applicability: All	**Reference(s):**	**Related Controls Requirement(s):**
ASSESSMENT PROCEDURE: IA-8.1		
Assessment Objective Determine if the information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users). **Assessment Methods And Objects** **Examine:** Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; list of information system accounts; other relevant documents or records.		

Incident Response (IR) – *Operational*

IR-1 – Incident Response Policy and Procedures (Low)

Control

The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:
a. A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.

Guidance

This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the incident response family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The incident response policy can be included as part of the general information security policy for the organization. Incident response procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the incident response policy.

Applicability: All	**Reference(s):** FISCAM: AC-5, AS-1, CP-2, SM-1, SM-3; HIPAA: 164.308(a)(6)(i); IRS-1075: 5.6.2.6#1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: IR-1.1

Assessment Objective

Determine if:
the organization develops and formally documents incident response policy;

the organization incident response policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented incident response policy to elements within the organization having associated incident response roles and responsibilities;

the organization develops and formally documents incident response procedures;

the organization incident response procedures facilitate implementation of the incident response policy and associated incident response controls;

the organization disseminates formal documented incident response procedures to elements within the organization having associated incident response roles and responsibilities;

the organization reviews/updates the incident response policy and procedures within every three hundred sixty-five (365) days.

Assessment Methods And Objects

Examine: Incident response policy and procedures; other relevant documents or records.

IR-2 – Incident Response Training (Low)

Control

The organization:
a. Trains personnel in their incident response roles and responsibilities with respect to the information system; and
b. Provides refresher training within every three hundred sixty-five (365) days.

Guidance

Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources. Incident response training implementation should:
(a) Identify employees with significant information security responsibilities and provide role-specific training in accordance with National Institute of Standards and Technology (NIST) standards and guidance:
(1) All users of CMS information systems must be exposed to security awareness materials at least annually. Users of CMS information systems include employees, contractors, students, guest researchers, visitors, and others who may need access to CMS information systems and applications.
(2) Executives must receive training in information security basics and policy level training in security planning and management.
(3) Program and functional managers must receive training in information security basics; management and implementation level training in security planning and system/application security management; and management and implementation level training in system/application life cycle management, risk management, and contingency planning.
(4) CIOs, IT security program managers, auditors, and other security-oriented personnel (e.g., system and network administrators, and system/application security officers) must receive training in information security basics and broad training in security planning, system and application security management, system/application life cycle management, risk management, and contingency planning.
(5) IT function management and operations personnel must receive training in information security basics; management and implementation level training in security planning and system/application security management; and management and implementation level training in system/ application life cycle management, risk management, and contingency planning.
(b) Provide the CMS information systems security awareness material/exposure outlined in NIST guidance on IT security awareness and training to all new employees before allowing them access to the systems.
(c) Provide information systems security refresher training for employees as frequently as determined necessary, based on the sensitivity of the information that the employees use or process.
(d) Provide training whenever there is a significant change in the information system environment or procedures or when an employee enters a new position that requires additional role-specific training.

Applicability: All	**Reference(s):** FISCAM: AC-5; IRS-1075: 5.6.2.6#2.1-2	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: IR-2.1

Assessment Objective

Determine if:
the organization identifies personnel with incident response roles and responsibilities with respect to the information system;

the organization provides incident response training to personnel with incident response roles and responsibilities with respect to the information system;

incident response training material addresses the procedures and activities necessary to fulfill identified organizational incident response roles and responsibilities;

the organization defines in the security plan, explicitly or by reference, the frequency of refresher incident response training and the frequency is at least annually;

the organization provides refresher incident response training in accordance with organization-defined frequency.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident response training; incident response training material; security plan; incident response plan; incident response training records; other relevant documents or records.

IR-4 – Incident Handling (Low)

Control

The organization:
a. Implements an incident handling capability using CMS Information Security Incident Handling and Breach Notification Procedures;
b. Coordinates incident handling activities with contingency planning activities; and
c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

Implementation Standard(s)

1. Document relevant information related to a security incident according to CMS Information Security Incident Handling and Breach Notification Procedures.
2. Preserve evidence through technical means, including secured storage of evidence media and "write" protection of evidence media. Use sound forensics processes and utilities that support legal requirements. Determine and follow chain of custody for forensic evidence.
3. Identify vulnerability exploited during a security incident. Implement security safeguards to reduce risk and vulnerability exploit exposure.

Guidance

Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

Applicability: All	**Reference(s):** FISCAM: AC-5; HIPAA: 164.308(a)(6)(ii); IRS-1075: 5.6.2.6#1, 5.6.2.6#2.3	**Related Controls Requirement(s):** AU-6, PE-6, SI-2

ASSESSMENT PROCEDURE: IR-4.1

Assessment Objective

Determine if:
the organization implements an incident handling capability for security incidents that includes:
- preparation;
- detection and analysis;
- containment;
- eradication;
- recovery;

the organization coordinates incident handling activities with contingency planning activities;

the organization incorporates lessons learned from ongoing incident handling activities into:
- incident response procedures;
- training;
- testing/exercises;

the organization implements the resulting changes to incident response procedures, training and testing/exercise accordingly.

the organization meets all the requirements specified in the applicable implementation standard(s).

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident handling; incident response plan; other relevant documents or records.

IR-5 – Incident Monitoring (Low)

Control

The organization tracks and documents information system security incidents.

Guidance

Documenting information system security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

Applicability: All	**Reference(s):** FISCAM: AC-5, SM-5; HIPAA: 164.308(a)(6)(ii); IRS-1075: 5.6.2.6#2.3	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: IR-5.1

Assessment Objective

Determine if the organization tracks and documents information system security incidents.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident monitoring; incident response records and documentation; incident response plan; other relevant documents or records.

IR-6 – Incident Reporting (Low)

Control

The organization:
a. Requires personnel to report suspected security incidents to the organizational incident response capability within timeframe established in the current CMS Information Security Incident Handling and Breach Analysis/Notification Procedure; and
b. Reports security incident information to designated authorities.

Guidance

The intent of this control is to address both specific incident reporting requirements within an organization and the formal incident reporting requirements for federal agencies and their subordinate organizations. The types of security incidents reported, the content and timeliness of the reports, and the list of designated reporting authorities are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. CMS requires that events and confirmed security incidents must be reported to the CMS IT Service Desk in accordance with established procedures.

Applicability: All	**Reference(s):** FISCAM: AC-5	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: IR-6.1

Assessment Objective

Determine if:
the organization requires personnel to report suspected security incidents to the organizational incident response capability within the timeframe established in the current CMS Information Security Incident Handling and Breach Analysis/Notification Procedure;

the organization reports security incident information to designated authorities.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident reporting; incident reporting records and documentation; security plan; incident response plan; other relevant documents or records.

IR-7 – Incident Response Assistance (Low)

Control

The organization provides an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

Guidance

Possible implementations of incident response support resources in an organization include a help desk or an assistance group and access to forensics services, when required. The CMS IT Service Desk is available to offer advice to users of a CMS information system.

Applicability: All	**Reference(s):** FISCAM: AC-5	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: IR-7.1

Assessment Objective

Determine if:
the organization provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents;

the incident response support resource is an integral part of the organization's incident response capability.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident response assistance; incident response plan; other relevant documents or records.

IR-8 – Incident Response Plan (Low)

Control

The organization:
a. Develops an incident response plan that:
- Provides the organization with a roadmap for implementing its incident response capability;
- Describes the structure and organization of the incident response capability;
- Provides a high-level approach for how the incident response capability fits into the overall organization;
- Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
- Defines reportable incidents;
- Provides metrics for measuring the incident response capability within the organization.
- Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
- Is reviewed and approved by designated officials within the organization;
b. Distributes copies of the incident response plan to incident response personnel and organizational elements;
c. Reviews the incident response plan within every three hundred sixty-five (365) days;
d. Revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and
e. Communicates incident response plan changes to incident response personnel and organizational elements.

Guidance

It is important that organizations have a formal, focused, and coordinated approach to responding to incidents. The organization's mission, strategies, and goals for incident response help determine the structure of its incident response capability.

Applicability: All	**Reference(s):**	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: IR-8.1

Assessment Objective

Determine if the organization develops an incident response plan that:
- provides the organization with a roadmap for implementing its incident response capability;
- describes the structure and organization of the incident response capability;
- provides a high-level approach for how the incident response capability fits into the overall organization;
- meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
- defines reportable incidents;
- provides metrics for measuring the incident response capability within the organization;
- defines the resources and management support needed to effectively maintain and mature an incident response capability;
- is reviewed and approved by designated officials within the organization.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident response assistance; incident response plan; other relevant documents or records.

ASSESSMENT PROCEDURE: IR-8.2

Assessment Objective

Determine if:
the organization defines, in the incident response plan, incident response personnel (identified by name and/or role) and organizational elements;

the organization distributes copies of the incident response plan to incident response personnel and organizational elements identified in the plan;

the organization reviews the incident response plan in accordance with the organization-defined frequency;

the organization revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;
the organization communicates incident response plan changes to incident response personnel and organizational elements identified in the plan.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident response assistance; incident response plan; other relevant documents or records.

Maintenance (MA) – *Operational*

MA-1 – System Maintenance Policy and Procedures (Low)

Control

The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:
a. A formal, documented information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.

Guidance

This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the system maintenance family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The information system maintenance policy can be included as part of the general information security policy for the organization. System maintenance procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system maintenance policy.

Applicability: All	**Reference(s):** FISCAM: AC-6, AS-1, CM-5, CP-2, SM-1, SM-3; HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.4#1.1, 5.6.2.4#1.2, 5.6.2.4#1.3	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: MA-1.1

Assessment Objective

Determine if:
the organization develops and formally documents system maintenance policy;

the organization system maintenance policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented system maintenance policy to elements within the organization having associated system maintenance roles and responsibilities;

the organization develops and formally documents system maintenance procedures;

the organization system maintenance procedures facilitate implementation of the system maintenance policy and associated system maintenance controls;

the organization disseminates formal documented system maintenance procedures to elements within the organization having associated system maintenance roles and responsibilities;

the organization reviews/updates the information system maintenance policy and procedures within every three hundred sixty-five (365) days.

Assessment Methods And Objects

Examine: Information system maintenance policy and procedures; other relevant documents or records.

MA-2 – Controlled Maintenance (Low)

Control

The organization:
a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;

b. Controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;
c. Requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;
d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; and
e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

Guidance

The control is intended to address the information security aspects of the organization's CMS information system maintenance program. Controlled maintenance includes, but is not limited to, scheduling, performing, testing, documenting, and reviewing records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.

Applicability: All; Optional for SS	**Reference(s):** FISCAM: AC-6, CP-2; IRS-1075: 5.6.2.4#1.1, 5.6.2.4#1.2, 5.6.2.4#1.3	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: MA-2.1

Assessment Objective

Determine if:
the organization schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;

the organization controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;

the organization requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;

the organization sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;

the organization checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

Assessment Methods And Objects

Examine: Information system maintenance policy; procedures addressing controlled maintenance for the information system; maintenance records; manufacturer/vendor maintenance specifications; equipment sanitization records; media sanitization records; other relevant documents or records.

MA-4 – Non-Local Maintenance (Low)

Control

The organization prohibits non-local CMS system maintenance unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization:
a. Monitors and controls non-local maintenance and diagnostic activities;
b. Allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;
c. Employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions;
d. Maintains records for non-local maintenance and diagnostic activities; and
e. Terminates all sessions and network connections when non-local maintenance is completed.

Implementation Standard(s)

1. If password-based authentication is used during remote maintenance, change the passwords following each remote maintenance service.

Guidance

Non-local maintenance and diagnostic activities are those activities conducted by individuals communicating through a network; either an external network (e.g., the Internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection. Identification and authentication techniques used in the establishment of non-local maintenance and diagnostic sessions are consistent with the network access requirements in IA-2. Strong authenticators include, for example, PKI where certificates are stored on a token protected by a password, passphrase, or biometric. Enforcing requirements in MA-4 is accomplished in part, by other controls.

Applicability: All	**Reference(s):** FISCAM: AC-4, SM-7; IRS-1075: 5.6.2.4#1.1, 5.6.2.4#1.2, 5.6.2.4#1.3	**Related Controls Requirement(s):** IA-2, MP-6

ASSESSMENT PROCEDURE: MA-4.1

Assessment Objective

Determine if:
the organization prohibits non-local CMS system maintenance unless explicitly authorized, in writing, by the CIO;

if authorized, the organization monitors and controls non-local maintenance and diagnostic activities;

if authorized, the organization documents, in the organizational policy and security plan for the information system, the acceptable conditions for allowing the use of non-local maintenance and diagnostic tools;

if authorized, the organization allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and as documented in the security plan;

if authorized, the organization employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions;

if authorized, the organization terminates all sessions and network connections when non-local maintenance is completed.

if authorized, the organization maintains records for non-local maintenance and diagnostic activities;

if authorized, the organization (or information system in certain cases) terminates all sessions and network connections when non-local maintenance or diagnostics is completed.

the organization meets all the requirements specified in the applicable implementation standard(s).

Assessment Methods And Objects

Examine: Information system maintenance policy; procedures addressing non-local maintenance for the information system; security plan; information system design documentation; information system configuration settings and associated documentation; maintenance records; other relevant documents or records.

MA-5 – Maintenance Personnel (Low)

Control

The organization:
a. Establishes a process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel; and
b. Ensures that personnel performing maintenance on the information system have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations.

Guidance

Individuals not previously identified in the information system, such as vendor personnel and consultants, may legitimately require privileged access to the system, for example, when required to conduct maintenance or diagnostic activities with little or no notice. Based on a prior assessment of risk, the organization may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for a very limited time period.

Applicability: All	**Reference(s):** FISCAM: CP-2, SM-7	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: MA-5.1

Assessment Objective

Determine if:
the organization establishes a process for maintenance personnel authorization;

the organization maintains a current list of authorized maintenance organizations or personnel;

personnel performing maintenance on the information system either have the required access authorizations or are supervised by designated organizational personnel with the required access authorizations and technical competence deemed necessary to supervise information system maintenance.

Assessment Methods And Objects

Examine: Information system maintenance policy; procedures addressing maintenance personnel; service provider contracts and/or service level agreements; list of authorized personnel; maintenance records; access control records; other relevant documents or records.

Media Protection (MP) – *Operational*

MP-1 – Media Protection Policy and Procedures (Low)

Control

The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:
a. A formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.

Guidance

This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the media protection family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The media protection policy can be included as part of the general information security policy for the organization. Media protection procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the media protection policy.

Applicability: All	**Reference(s):** FISCAM: AC-6, AS-1, SM-1, SM-3; HIPAA: 164.310(d)(1); IRS-1075: 4.6#1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: MP-1.1

Assessment Objective

Determine if:
the organization develops and formally documents media protection policy;

the organization media protection policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented media protection policy to elements within the organization having associated media protection roles and responsibilities;

the organization develops and formally documents media protection procedures;

the organization media protection procedures facilitate implementation of the media protection policy and associated media protection controls;

the organization disseminates formal documented media protection procedures to elements within the organization having associated media protection roles and responsibilities.

the organization reviews/updates the media protection policy and procedures within every three hundred sixty-five (365) days.

Assessment Methods And Objects

Examine: Media protection policy and procedures; other relevant documents or records.

MP-2 – Media Access (Low)

Control

The organization restricts access to CMS sensitive digital and non-digital media to authorized individuals using automated mechanisms to control access to media storage areas.

Guidance

Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to mobile computing and communications devices with information storage capability (e.g., notebook/laptop

computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). An organizational assessment of risk guides the selection of media and associated information contained on that media requiring restricted access. Organizations document in policy and procedures, the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access. Fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls where the media resides provide adequate protection.

Applicability: All	**Reference(s):** FISCAM: AC-4, AC-6, BP-3; HIPAA: 164.308(a)(3)(ii)(A), 164.312(c)(1); IRS-1075: 4.6#1, 6.3.3#1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: MP-2.1

Assessment Objective

Determine if:
the organization defines:
- digital and non-digital media requiring restricted access;
- individuals authorized to access the media;
- security measures taken to restrict access;

the organization restricts access to organization-defined information system media to organization-defined authorized individuals using organization-defined security measures.

Assessment Methods And Objects

Examine: Information system media protection policy; procedures addressing media access; access control policy and procedures; physical and environmental protection policy and procedures; media storage facilities; access control records; other relevant documents or records.

MP-6 – Media Sanitization (Low)

Control

The organization:
a. Sanitizes information system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse; and
b. Employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information.

Implementation Standard(s)

1. Finely shred, using a minimum of cross-cut shredding, hard-copy documents, using approved equipment, techniques, and procedures.

Guidance

This control applies to all media subject to disposal or reuse, whether or not considered removable. Sanitization is the process used to remove information from information system media such that there is reasonable assurance that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, and destroying media information, prevent the disclosure of sensitive information to unauthorized individuals when such media is reused or released for disposal. The organization uses its discretion on the employment of sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on CMS or individuals if released for reuse or disposal.

Applicability: All	**Reference(s):** FISCAM: AC-4; HIPAA: 164.310(d)(2)(i), 164.310(d)(2)(ii); IRS-1075: 4.7.3#1.3, 5.3#3, 6.3.4#1, 8.3#1, 8.3#2	**Related Controls Requirement(s):** MA-4

ASSESSMENT PROCEDURE: MP-6.1

Assessment Objective

Determine if:
the organization sanitizes information system media both digital and non-digital prior to:
- disposal;
- release out of organizational control; or
- release for reuse;

the organization employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information.

the organization meets all the requirements specified in the applicable implementation standard(s).

Assessment Methods And Objects

Examine: Information system media protection policy; procedures addressing media sanitization and disposal; media sanitization records; audit records; other relevant documents or records.

Physical and Environmental Protection (PE) – *Operational*

PE-1 – Physical and Environmental Protection Policy and Procedures (Low)		
Control The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days: a. A formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.		
Guidance This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the physical and environmental protection family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The physical and environmental protection policy can be included as part of the general information security policy for the organization. Physical and environmental protection procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the physical and environmental protection policy.		
Applicability: All	**Reference(s):** FISCAM: AC-6, AS-1, AS-2, CP-2, SM-1, SM-3; HIPAA: 164.310(a)(1), 164.310(a)(2)(ii), 164.312(c)(1); IRS-1075: 4.6#1	**Related Controls Requirement(s):**
ASSESSMENT PROCEDURE: PE-1.1		
Assessment Objective Determine if: the organization develops and formally documents physical and environmental protection policy; the organization physical and environmental protection policy addresses: - purpose; - scope; - roles and responsibilities; - management commitment; - coordination among organizational entities; - compliance; the organization disseminates formal documented physical and environmental protection policy to elements within the organization having associated physical and environmental protection roles and responsibilities; the organization develops and formally documents physical and environmental protection procedures; the organization physical and environmental protection procedures facilitate implementation of the physical and environmental protection policy and associated physical and environmental protection controls; the organization disseminates formal documented physical and environmental protection procedures to elements within the organization having associated physical and environmental protection roles and responsibilities; the organization reviews/updates the physical and environmental protection policy and procedures within every three hundred sixty-five (365) days.		
Assessment Methods And Objects **Examine:** Physical and environmental protection policy and procedures; other relevant documents or records.		

PE-2 – Physical Access Authorizations (Low)

Control

The organization:
a. Develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);
b. Issues authorization credentials;
c. Reviews and approves the access list and authorization credentials in accordance with the frequency specified in Implementation Standard 1, removing from the access list personnel no longer requiring access.

Implementation Standard(s)

1. Review and approve lists of personnel with authorized access to facilities containing information systems at least once every three hundred sixty-five (365) days.

Guidance

Authorization credentials include, for example, badges, identification cards, and smart cards.

Applicability: All	**Reference(s):** FISCAM: AC-6	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PE-2.1

Assessment Objective

Determine if:
the organization identifies areas within the facility that are publicly accessible;

the organization develops and keeps current lists of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);

the organization issues authorization credentials (e.g., badges, identification cards, smart cards).

the organization reviews and approves the access list and authorization credentials in accordance with the frequency specified in Implementation Standard 1, removing from the access list personnel no longer requiring access.

the organization meets all the requirements specified in the applicable implementation standard(s).

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access authorizations; security plan; authorized personnel access list; authorization credentials; list of areas that are publicly accessible; other relevant documents or records.

PE-3 – Physical Access Control (Low)

Control

The organization:
a. Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible);
b. Verifies individual access authorizations before granting access to the facility;
c. Controls entry to the facility containing the information system using physical access devices and/or guards;
d. Controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk;
e. Controls access authorization lists to secure areas;
f. Secures keys, combinations, and other physical access devices;
g. Inventories physical access devices within every three hundred sixty-five (365) days; and
h. Changes combinations and keys when keys are lost, combinations are compromised, or individuals are transferred or terminated.

Implementation Standard(s)

1. Control data center/facility access by use of door and window locks.
2. Store and operate servers in physically secure environments protected from unauthorized access.

Guidance

The organization determines the types of guards needed, for example, professional physical security staff or other personnel such as administrative staff or information system users, as deemed appropriate. Physical access devices include, for example, keys, locks, combinations, and card readers. Workstations and associated peripherals connected to (and part of) a CMS information system may be located in areas designated as publicly accessible with access to such devices being safeguarded.

Applicability: All	**Reference(s):** FISCAM: AC-6, SD-1, SM-4; HIPAA: 164.310(a)(2)(iii), 164.310(c); IRS-1075: 4.2#2, 4.6#1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PE-3.1

Assessment Objective

Determine if:
the organization enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible);

the organization verifies individual access authorizations before granting access to the facility;

the organization controls entry to the facility containing the information system using physical access devices (e.g., keys, locks, combinations, card readers) and/or guards;

the organization controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk;

the organization secures keys, combinations, and other physical access devices;

the organization inventories physical access devices within every three hundred sixty-five (365) days;

the organization changes combinations and keys periodically; and when keys are lost, combinations are compromised, or individuals are transferred or terminated.

the organization meets all the requirements specified in the applicable implementation standard(s).

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing physical access control; security plan; physical access control logs or records; inventory records of physical access devices; records of key and lock combination changes; storage locations for physical access devices; other relevant documents or records.

PE-6 – Monitoring Physical Access (Low)

Control

The organization:
a. Monitors physical access to the information system to detect and respond to physical security incidents;
b. Reviews physical access logs in accordance with the frequency specified in Implementation Standard 1; and
c. Coordinates results of reviews and investigations with the organization's incident response capability.

Implementation Standard(s)

1. Review physical access logs every at least once every three (3) months.

Guidance

Investigation of and response to detected physical security incidents, including apparent security violations or suspicious physical access activities, are part of the organization's incident response capability.

Applicability: All	**Reference(s):** FISCAM: AC-5, AC-6, SM-5	**Related Controls Requirement(s):** IR-4

ASSESSMENT PROCEDURE: PE-6.1		
Assessment Objective Determine if: the organization monitors physical access to the information system to detect and respond to physical security incidents; the organization reviews physical access logs in accordance with the organization-defined frequency; the organization coordinates results of reviews and investigations with the organization's incident response capability. the organization meets all the requirements specified in the applicable implementation standard(s). **Assessment Methods And Objects** **Examine:** Physical and environmental protection policy; procedures addressing physical access monitoring; security plan; physical access logs or records; other relevant documents or records.		
PE-7 – Visitor Control (Low)		
Control The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.		
Guidance Individuals (to include organizational employees, contract personnel, and others) with permanent authorization credentials for the facility are not considered visitors.		
Applicability: All	**Reference(s):** FISCAM: AC-6; HIPAA: 164.310(a)(2)(iii)	**Related Controls Requirement(s):**
ASSESSMENT PROCEDURE: PE-7.1		
Assessment Objective Determine if the organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible. **Assessment Methods And Objects** **Examine:** Physical and environmental protection policy; procedures addressing visitor access control; visitor access control logs or records; other relevant documents or records.		
PE-8 – Access Records (Low)		
Control The organization: a. Maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); and b. Closes and reviews visitor access records monthly.		
Guidance Visitor access records include, for example, name/organization of the person visiting, signature of the visitor, form(s) of identification, date of access, time of entry and departure, purpose of visit, and name/organization of person visited.		
Applicability: All	**Reference(s):** FISCAM: AC-6	**Related Controls Requirement(s):**
ASSESSMENT PROCEDURE: PE-8.1		
Assessment Objective Determine if: the organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly		

accessible);

the organization reviews the visitor access records in accordance with the organization-defined frequency.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing facility access records; security plan; facility access control records; other relevant documents or records.

PE-12 – Emergency Lighting (Low)

Control

The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

Guidance

This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

Applicability: All	**Reference(s):** FISCAM: AC-6, CP-2	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PE-12.1

Assessment Objective

Determine if:
the organization employs automatic emergency lighting for the information system that activates in the event of a power outage or disruption;

the organization employs automatic emergency lighting for the information system that covers emergency exits and evacuation routes within the facility;

the organization maintains the automatic emergency lighting for the information system.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing emergency lighting; emergency lighting documentation; emergency lighting test records; emergency exits and evacuation routes; other relevant documents or records.

PE-13 – Fire Protection (Low)

Control

The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

Guidance

Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors. This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

Applicability: All	**Reference(s):** FISCAM: CP-2	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PE-13.1

Assessment Objective

Determine if:
the organization employs fire suppression and detection devices/systems for the information system that are supported by an independent energy source;

the organization maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing fire protection; fire suppression and detection devices/systems; fire suppression and detection

devices/systems documentation; test records of fire suppression and detection devices/systems; other relevant documents or records.

PE-14 – Temperature and Humidity Controls (Low)

Control

The organization:
a. Maintains temperature and humidity levels within the facility where the information system resides within acceptable vendor-recommended levels; and
b. Monitors temperature and humidity levels.

Implementation Standard(s)

1. Evaluate the level of alert and follow prescribed guidelines for that alert level.

Guidance

This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

Applicability: All	**Reference(s):** FISCAM: AC-6, CP-2	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PE-14.1

Assessment Objective

Determine if:
the organization defines the acceptable temperature and humidity levels within the facility where the information system resides;

the organization maintains temperature and humidity levels within the facility where the information system resides in accordance with organization-defined acceptable levels;

the organization defines the frequency to monitor temperature and humidity levels;

the organization monitors the temperature and humidity levels within the facility where the information system resides in accordance with the organization-defined frequency.

the organization meets all the requirements specified in the applicable implementation standard(s).

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing temperature and humidity control; security plan; temperature and humidity controls; facility housing the information system; temperature and humidity controls documentation; temperature and humidity records; other relevant documents or records.

PE-15 – Water Damage Protection (Low)

Control

The organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.

Guidance

This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

Applicability: All	**Reference(s):** FISCAM: AC-6, CP-2	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PE-15.1

Assessment Objective

Determine if:
the organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible and working properly;

key personnel within the organization have knowledge of the master water shutoff values.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing water damage protection; facility housing the information system; master shutoff valves; list of key personnel with knowledge of location and activation procedures for master shutoff valves for the plumbing system; master shutoff valve documentation; other relevant documents or records.

PE-16 – Delivery and Removal (Low)

Control

The organization authorizes, monitors, and controls the flow of CMS information system-related components entering and exiting the facility and maintains records of those items.

Guidance

Effectively enforcing authorizations for entry and exit of information system components may require restricting access to delivery areas and possibly isolating the areas from the information system and media libraries.

Applicability: All	**Reference(s):** FISCAM: AC-6	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PE-16.1

Assessment Objective

Determine if:
the organization authorizes, monitors, and controls organization-defined information system components entering and exiting the facility;

the organization maintains records of information system components entering and exiting the facility.

Assessment Methods And Objects

Examine: Physical and environmental protection policy; procedures addressing delivery and removal of information system components from the facility; security plan; facility housing the information system; records of items entering and exiting the facility; other relevant documents or records.

Planning (PL) – *Management*

PL-1 – Security Planning Policy and Procedures (Low)

Control

The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:
a. A formal, documented security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.

Guidance

This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the security planning family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The security planning policy addresses the overall policy requirements for confidentiality, integrity, and availability and can be included as part of the general information security policy for the organization. Security planning procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the security planning policy.

Applicability: All	**Reference(s):** FISCAM: AS-1, SM-1, SM-3; HIPAA: 164.308(a)(1)(i), 164.316(a); HSPD 7: J(35); IRS-1075: 5.6.1.2#1.1-2	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PL-1.1

Assessment Objective

Determine if:
the organization develops and formally documents security planning policy;

the organization security planning policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented security planning policy to elements within the organization having associated security planning roles and responsibilities;

the organization develops and formally documents security planning procedures;

the organization security planning procedures facilitate implementation of the security planning policy and associated security planning controls;

the organization disseminates formal documented security planning procedures to elements within the organization having associated security planning roles and responsibilities;

the organization reviews/updates the security planning policy and procedures within every three hundred sixty-five (365) days.

Assessment Methods And Objects

Examine: Security planning policy and procedures; other relevant documents or records.

PL-2 – System Security Plan (SSP) (Low)

Control

The organization:
a. Develops a security plan for the information system that:
- Is consistent with the CMS System Security Plan (SSP) Procedure;
- Is consistent with the organization's enterprise architecture;

- Explicitly defines the authorization boundary for the system;
- Describes the operational context of the information system in terms of missions and business processes;
- Provides the security categorization of the information system including supporting rationale;
- Describes the operational environment for the information system;
- Describes relationships with or connections to other information systems;
- Provides an overview of the security requirements for the system;
- Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and
- Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;

b. Reviews the security plan for the information system within every three hundred sixty-five (365) days; and

c. Updates the plan, minimally every three (3) years, to address current conditions or whenever:
- There are significant changes to the information system/environment of operation that affect security;
- Problems are identified during plan implementation or security control assessments:
- When the data sensitivity level increases;
- After a serious security violation due to changes in the threat environment; or
- Before the previous security authorization expires.

Guidance

The security plan contains sufficient information (including specification of parameters for assignment and selection statements in security controls either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a subsequent determination of risk to CMS operations and assets, individuals, other organizations, and the Nation if the plan is implemented as intended.
All CMS information systems and major applications are covered by an SSP, which is compliant with current CMS SSP Procedures.

Applicability: All	**Reference(s):** FISCAM: AS-1, AS-2, CP-1, CP-2, SM-1; HIPAA: 164.316(a); HSPD 7: J(35); IRS-1075: 4.1#1, 5.3#4, 5.3#5, 5.6.1.2#1.3	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PL-2.1

Assessment Objective

Determine if:
the organization develops a security plan for the information system that:
- is consistent with the organization's enterprise architecture;
- explicitly defines the authorization boundary for the system;
- describes the operational context of the information system in terms of mission and business processes;
- provides the security categorization of the information system including supporting rationale;
- describes the operational environment for the information system;
- describes relationships with or connections to other information systems;
- provides an overview of the security requirements for the system;
- describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplemental decisions;
- is reviewed and approved by the authorizing official or designated representative prior to plan implementation;

the organization defines the frequency of security plan reviews;

the organization reviews the security plan in accordance with the organization-defined frequency, minimally every three (3) years;

the organization updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.

Assessment Methods And Objects

Examine: Security planning policy; procedures addressing security plan development and implementation; procedures addressing security plan reviews and updates; enterprise architecture documentation; security plan for the information system; records of security plan reviews and updates; other relevant documents or records.

PL-3 – System Security Plan Update (Low)

Control

[Withdrawn: Incorporated into PL-2].

PL-4 – Rules of Behavior (ROB) (Low)

Control

The organization:
a. Establishes and makes readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to information, information system, and network use; and
b. Receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.

Guidance

The organization considers different sets of rules based on user roles and responsibilities, for example, differentiating between the rules that apply to privileged users and rules that apply to general users. Electronic signatures are acceptable for use in acknowledging rules of behavior.
ROBs are aligned with DHHS requirements posted at http://hhs.gov/ocio/policy/2008-0001.003s.html, and made readily available.

Applicability: All	**Reference(s):** FISCAM: CP-2, SM-4; HIPAA: 164.306(a)(4); HSPD 7: J(35); IRS-1075: 5.6.1.2#1.5	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PL-4.1

Assessment Objective

Determine if:
the organization establishes the rules that describe information system user responsibilities and expected behavior with regard to information and information system usage;

the organization makes the rules available to all information system users;

the organization receives a signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.

Assessment Methods And Objects

Examine: Security planning policy; procedures addressing rules of behavior for information system users; rules of behavior; other relevant documents or records.

PL-5 – Privacy Impact Assessment (PIA) (Low)

Control

The organization conducts a Privacy Impact Assessment (PIA) on the information system in accordance with OMB policy.

Applicability: All; Optional for ABMAC, COB, CWF, DC, DMEMAC, EDC, PSC, PartA, PartB, QIC, RAC, SS, ZPIC	**Reference(s):** FISCAM: SM-5; HSPD 7: J(35)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PL-5.1

Assessment Objective

Determine if:
the organization conducts a privacy impact assessment on the information system;

the privacy impact assessment is in accordance with OMB policy.

Assessment Methods And Objects

Examine: Security planning policy; procedures addressing privacy impact assessments on the information system; privacy impact assessment; other relevant documents or records.

Personnel Security (PS) – *Operational*

PS-1 – Personnel Security Policy and Procedures (Low)

Control

The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:
a. A formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.

Guidance

This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the personnel security family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The personnel security policy can be included as part of the general information security policy for the organization. Personnel security procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the personnel security policy.

Applicability: All	**Reference(s):** FISCAM: AS-1, SD-2, SM-1, SM-3, SM-4; IRS-1075: 5.6.2.1#1.1-2	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PS-1.1

Assessment Objective

Determine if:
the organization develops and formally documents personnel security policy;

the organization personnel security policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented personnel security policy to elements within the organization having associated personnel security roles and responsibilities;

the organization develops and formally documents personnel security procedures;

the organization personnel security procedures facilitate implementation of the personnel security policy and associated personnel security controls;

the organization disseminates formal documented personnel security procedures to elements within the organization having associated personnel security roles and responsibilities;

the organization reviews/updates the personnel security policy and procedures within every three hundred sixty-five (365) days.

Assessment Methods And Objects

Examine: Personnel security policy and procedures, other relevant documents or records.

PS-2 – Position Categorization (Low)

Control

The organization:
a. Assigns a criticality/sensitivity risk designation to all positions;
b. Establishes screening criteria for individuals filling those positions; and
c. Reviews and revises position criticality/sensitivity risk designations within every three hundred sixty-five (365) days.

Guidance

Position risk designations are consistent with Office of Personnel Management policy and guidance. The screening criteria include explicit information security role appointment requirements (e.g., training, security clearance).

Applicability: All	**Reference(s):** FISCAM: SD-1, SD-2, SM-4; IRS-1075: 5.6.2.1#1.3	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PS-2.1

Assessment Objective

Determine if:
the organization assigns a risk designations to all positions within the organization;

the organization establishes a screening criteria for individuals filling organizational positions;

the organization defines in the security plan, explicitly or by reference, the frequency of risk designation reviews and updates for organizational positions;

the organization reviews/revises position risk designations within every three hundred sixty-five (365) days.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing position categorization; appropriate codes of federal regulations; list of risk designations for organizational positions; security plan; records of risk designation reviews and updates; other relevant documents or records.

PS-3 – Personnel Screening (Low)

Control

The organization:
a. Screens individuals prior to authorizing access to the information system; and
b. Rescreens individuals periodically, consistent with the criticality/sensitivity rating of the position.

Implementation Standard(s)

1. Perform criminal history check for all persons prior to employment.
2. Require appropriate personnel to obtain and hold a low-risk security clearance as defined in DHHS Personnel Security/Suitability Handbook.

Guidance

Screening and rescreening are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidance, and the criteria established for the risk designation of the assigned position.
For prospective employees, references background checks are performed before issuance of a User ID. Security agreements are required for employees and contractors assigned to work with mission critical information.

Applicability: All	**Reference(s):** FISCAM: AC-6, SM-4, SM-7; IRS-1075: 5.6.2.1#1.4	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PS-3.1

Assessment Objective

Determine if:
the organization screens individuals prior to authorizing access to the information system;

the organization rescreens individuals periodically, consistent with the criticality/sensitivity rating of the position;

the personnel screening is consistent with 5 CFR 731.106, OPM policy, regulations, and guidance, FIPS 201 and NIST Special Publications 800-73, 800-76, and 800-78, and the criteria established for the risk designation for the assigned position.

the organization meets all the requirements specified in the applicable implementation standard(s).

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing personnel screening; records of screened personnel; security plan; other relevant documents or records.

PS-4 – Personnel Termination (Low)

Control

The organization, upon termination of individual employment:
a. Revokes system and physical access immediately following employee termination;
b. Conducts exit interviews;
c. Retrieves all security-related CMS information system-related property;
d. Retains access to CMS information and information systems formerly controlled by terminated individual; and
e. Immediately escorts employees terminated for cause out of the organization.

Implementation Standard(s)

1. System access must be revoked immediately following employee termination.

Guidance

Information system-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that individuals understand any security constraints imposed by being former employees and that proper accountability is achieved for all CMS information system-related property. Exit interviews may not be possible for some employees (e.g., in the case of job abandonment, some illnesses, and nonavailability of supervisors). Exit interviews are important for individuals with security clearances. Timely execution of this control is particularly essential for employees or contractors terminated for cause. Appropriate personnel have access to official records created by the terminated employee that are stored on CMS information systems.

Applicability: All	**Reference(s):** FISCAM: SM-4; HIPAA: 164.308(a)(3)(ii)(C); IRS-1075: 5.6.2.1#1.5	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PS-4.1

Assessment Objective

Determine if:
the organization terminates information system access upon termination of individual employment;

the organization conducts exit interviews of terminated personnel;

the organization retrieves all security-related CMS information system-related property from terminated personnel;

the organization, upon termination of individual employment, retrieves all security-related CMS information system-related property;

the organization, upon termination of individual employment, retains access to CMS information and information systems formerly controlled by terminated individual;

the organization, upon termination of individual employment, immediately escorts employees terminated for cause out of the organization.

the organization meets all the requirements specified in the applicable implementation standard(s).

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing personnel termination; records of personnel termination actions; list of information system accounts; other relevant documents or records.

PS-5 – Personnel Transfer (Low)

Control

The organization reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization and initiates the following transfer or reassignment actions during the formal transfer process:
a. Re-issuing appropriate CMS information system-related property (e.g., keys, identification cards, building passes);
b. Notification to security management;
c. Closing obsolete accounts and establishing new accounts; and
d. Revocation of all system access privileges (if applicable).

Guidance

This control applies when the reassignment or transfer of an employee is permanent or of such an extended duration as to make the actions warranted. In addition the organization defines the actions appropriate for the type of reassignment or transfer; whether permanent or temporary. Actions that may be required when personnel are transferred or reassigned to other positions within the organization include, for example: (i) returning old and issuing new keys, identification cards, and building passes; (ii) closing previous information system accounts and establishing new accounts; (iii) changing information system access authorizations; and (iv) providing for access to official records to which the employee had access at the previous work location and in the previous information system accounts.

Applicability: All	**Reference(s):** FISCAM: SM-4; IRS-1075: 5.6.2.1#1.6	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PS-5.1

Assessment Objective

Determine if:
the organization reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization;

the organization defines the transfer or reassignment actions and the time period within which the actions must occur following formal transfer or reassignment;

the organization initiates the organization-defined transfer or reassignment actions within an organization-defined time period following formal transfer or reassignment.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing personnel transfer; security plan; records of personnel transfer actions; list of information system and facility access authorizations; other relevant documents or records.

PS-6 – Access Agreements (Low)

Control

The organization:
a. Ensures that individuals requiring access to CMS information or information systems sign appropriate access agreements prior to being granted access; and
b. Reviews/updates the access agreements as part of the system security authorization or when a contract is renewed or extended.

Guidance

Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with the information system to which access is authorized. Electronic signatures are acceptable for use in acknowledging access agreements unless specifically prohibited by organizational policy.

Applicability: All	**Reference(s):** FISCAM: AC-6, AS-1, SD-1, SD-2, SM-4; IRS-1075: 5.6.2.1#1.7	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PS-6.1

Assessment Objective

Determine if:
the organization identifies appropriate access agreements for individuals requiring access to CMS information and information systems;

individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access;

the organization defines in the security plan, explicitly or by reference, the frequency of reviews/updates for access agreements;

the organization reviews/updates the access agreements in accordance with the organization-defined frequency.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing access agreements for organizational information and information systems; security plan; access agreements; records of access agreement reviews and updates; other relevant documents or records.

PS-7 – Third-Party Personnel Security (Low)

Control

The organization:
a. Establishes personnel security requirements including security roles and responsibilities for third-party providers;
b. Documents personnel security requirements; and
c. Monitors provider compliance.

Implementation Standard(s)

1. Regulate the access provided to contractors and define security requirements for contractors. Contractors must be provided with minimal system and physical access, and must agree to and support the CMS information security requirements. The contractor selection process must assess the contractor's ability to adhere to and support CMS' information security policies and standards.

Guidance

Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. The organization explicitly includes personnel security requirements in acquisition-related documents. Security requirements include provisions for security clearances, background checks, required expertise, defined security roles and responsibilities, and confidentiality agreements.

Applicability: All	**Reference(s):** FISCAM: AC-6, AS-1, SD-1, SM-4, SM-7; IRS-1075: 5.6.2.1#1.8	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PS-7.1

Assessment Objective

Determine if:
the organization establishes personnel security requirements, including security roles and responsibilities, for third-party providers;

the organization documents personnel security requirements for third-party providers;

the organization monitors third-party provider compliance with personnel security requirements.

the organization meets all the requirements specified in the applicable implementation standard(s).

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing third-party personnel security; list of personnel security requirements; acquisition documents; compliance monitoring process; other relevant documents or records.

PS-8 – Personnel Sanctions (Low)

Control

The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.

Guidance

The sanctions process is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The process is described in access agreements and can be included as part of the general personnel policies and procedures for the organization.

Applicability: All	**Reference(s):** FISCAM: AC-5, SD-2, SM-4; HIPAA: 164.308(a)(1)(ii)(C)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: PS-8.1

Assessment Objective

Determine if the organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.

Assessment Methods And Objects

Examine: Personnel security policy; procedures addressing personnel sanctions; rules of behavior; records of formal sanctions; other relevant documents or records.

Risk Assessment (RA) – *Management*

RA-1 – Risk Assessment Policy and Procedures (Low)

Control

The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:
a. A formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.

Guidance

This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the risk assessment family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The risk assessment policy can be included as part of the general information security policy for the organization. Risk assessment procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the risk assessment policy.

Applicability: All	**Reference(s):** FISCAM: AS-1, SM-1, SM-2, SM-3; HIPAA: 164.306(a)(2), 164.316(a); IRS-1075: 5.6.1.1#1.1-2	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: RA-1.1

Assessment Objective

Determine if:
the organization develops and formally documents risk assessment policy;

the organization risk assessment policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented risk assessment policy to elements within the organization having associated risk assessment roles and responsibilities;

the organization develops and formally documents risk assessment procedures;

the organization risk assessment procedures facilitate implementation of the risk assessment policy and associated risk assessment controls;

the organization disseminates formal documented risk assessment procedures to elements within the organization having associated risk assessment roles and responsibilities;

the organization reviews/updates the risk assessment policy and procedures within every three hundred sixty-five (365) days.

Assessment Methods And Objects

Examine: Risk assessment policy and procedures; other relevant documents or records.

RA-2 – Security Categorization (Low)

Control

The organization:
a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and
c. Ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.

Guidance

A clearly defined authorization boundary is a prerequisite for an effective security categorization. Security categorization describes the potential adverse impacts to CMS operations, CMS assets, and individuals should the information and information system be comprised through a loss of confidentiality, integrity, or availability. The organization conducts the security categorization process as an organization-wide activity with the involvement of the CMS CIO, CISO, Business Owner, senior information security officer, and information owners/stewards. The security categorization process facilitates the creation of an inventory of information assets, and in conjunction with CM-8, a mapping to the information system components where the information is processed, stored, and transmitted.
All CMS information systems categorized as High or Moderate are considered sensitive or to contain sensitive information. All CMS information systems categorized as Low are considered non-sensitive or to contain non-sensitive information. Organizations implement the minimum security requirements and controls as established in the current CMS Information Security ARS Standard, based on the system security categorization.

Applicability: All	**Reference(s):** FISCAM: CP-1, SM-2; HSPD 7: D(8); IRS-1075: 4.1#2	**Related Controls Requirement(s):** MP-4, SC-7

ASSESSMENT PROCEDURE: RA-2.1

Assessment Objective

Determine if:
the organization categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

the organization documents the security categorization results (including supporting rationale) in the security plan for the information system;

the CMS authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

Assessment Methods And Objects

Examine: Risk assessment policy; procedures addressing security categorization of organizational information and information systems; security planning policy and procedures; security plan; security categorization documentation; other relevant documents or records.

RA-3 – Risk Assessment (Low)

Control

The organization:
a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
b. Documents risk assessment results in accordance with the CMS Information Security (IS) Risk Assessment (RA) Procedures;
c. Reviews risk assessment results within every three hundred sixty-five (365) days; and
d. Updates the risk assessment within every three (3) years or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security or authorization state of the system.

Guidance

A clearly defined authorization boundary is a prerequisite for an effective risk assessment. Risk assessments take into account vulnerabilities, threat sources, and security controls planned or in place to determine the level of residual risk posed to CMS operations and assets, individuals, other organizations, and the Nation based on the operation of the information system. Risk assessments also take into account risk posed to CMS operations, CMS assets, or individuals from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing CMS information systems, outsourcing entities).
In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. As such, organizational assessments of risk also address public access to federal information systems. The General Services Administration provides tools supporting that portion of the risk assessment dealing with public access to federal information systems.
Risk assessments can be conducted by organizations at various steps in the Risk Management Framework including: information system categorization; security control selection; security control implementation; security control assessment; information system authorization; and security control monitoring. RA-3 is a noteworthy security control in that the control must be partially implemented prior to the implementation of other controls in order to complete the first two steps in the Risk Management Framework. Risk assessments can play an important role in the security control selection process during the application of tailoring guidance for security control baselines and when considering supplementing the baselines with additional security controls or control enhancements.

Applicability: All	Reference(s): FISCAM: AC-6, AS-1, AS-5, CP-1, CP-2, SM-2; HIPAA: 164.306(a)(2), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.316(a); HSPD 7: D(8), F(19); IRS-1075: 5.6.1.1#1.3, 6.3.3#2	Related Controls Requirement(s):

ASSESSMENT PROCEDURE: RA-3.1

Assessment Objective

Determine if:
the organization conducts an assessment of risk of the information system and the information it processes, stores, or transmits that includes the likelihood and magnitude of harm, from the unauthorized:
- access;
- use;
- disclosure;
- disruption;
- modification; or
- destruction;

the organization documents risk assessment results in accordance with the CMS IS RA Procedures;

the organization reviews risk assessment results within every three hundred sixty-five (365) days;

the organization updates the risk assessment within every three (3) years or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security or authorization state of the system.

Assessment Methods And Objects

Examine: Risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; security plan; risk assessment; other relevant documents or records.

RA-4 – Risk Assessment Update (Low)

Control

[Withdrawn: Incorporated into RA-3].

RA-5 – Vulnerability Scanning (Low)

Control

The organization:
a. Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:
- Enumerating platforms, software flaws, and improper configurations;
- Formatting and making transparent, checklists and test procedures; and
- Measuring vulnerability impact;
b. Analyzes vulnerability scan reports and results from security control assessments;
c. Remediates legitimate vulnerabilities based on the Business Owner's risk prioritization in accordance with an organizational assessment of risk; and
d. Shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization on a "need to know" basis to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

Implementation Standard(s)

1. Scans for vulnerabilities in the information system and hosted applications within every ninety (90) days and when new vulnerabilities potentially affecting the system/applications are identified and reported.
2. Perform external network penetration testing and conduct enterprise security posture review as needed but no less than once within every three hundred sixty-five (365) days, in accordance with CMS IS procedures.

Guidance

The security categorization of the information system guides the frequency and comprehensiveness of the vulnerability scans. Vulnerability analysis for custom software and applications may require additional, more specialized techniques and approaches (e.g., web-based application scanners, source code reviews, source code analyzers). Vulnerability scanning includes scanning for specific functions, ports, protocols, and services that should not be accessible to users or devices and for improperly configured or incorrectly operating information flow mechanisms. The organization considers using tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to test for the presence of vulnerabilities. The Common Weakness Enumeration (CWE) and the National Vulnerability Database (NVD) are also excellent sources for vulnerability information. In addition, security control assessments such as red team exercises are another source of potential vulnerabilities for which to scan.

Applicability: All	**Reference(s):** FISCAM: CM-5, SM-5; HIPAA: 164.306(a)(2); HSPD 7: F(19), G(24)	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: RA-5.1

Assessment Objective

Determine if:
the organization employs vulnerability scanning tools and techniques that use standards to promote interoperability among tools and automate parts of the vulnerability management process that focus on:
- enumerating platforms, software flaws, and improper configurations;
- formatting/and making transparent checklists and test procedures;
- measuring vulnerability impact;

the organization analyzes vulnerability scan reports and results from security control assessments;

the organization remediates legitimate vulnerabilities based on the Business Owner's risk prioritization in accordance with an organizational assessment of risk;

the organization shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

Assessment Methods And Objects

Examine: Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; security plan; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records.

System and Services Acquisition (SA) – *Management*

SA-1 – System and Services Acquisition Policy and Procedures (Low)

Control

The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:
a. A formal, documented system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.

Guidance

This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the system and services acquisition family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The system and services acquisition policy can be included as part of the general information security policy for the organization. System and services acquisition procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system and services acquisition policy.

Applicability: All	**Reference(s):** FISCAM: AS-1, SM-1, SM-3; IRS-1075: 5.6.1.3#1.1-2	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SA-1.1

Assessment Objective

Determine if:
the organization develops and formally documents system services and acquisition policy;

the organization system services and acquisition policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented system services and acquisition policy to elements within the organization having associated system services and acquisition roles and responsibilities;

the organization develops and formally documents system services and acquisition procedures;

the organization system services and acquisition procedures facilitate implementation of the system and services acquisition policy and associated system services and acquisition controls;

the organization disseminates formal documented system services and acquisition procedures to elements within the organization having associated system services and acquisition roles and responsibilities;

the organization reviews/updates the system services and acquisition policy and procedures within every three hundred sixty-five (365) days.

Assessment Methods And Objects

Examine: System and services acquisition policy and procedures; other relevant documents or records.

SA-2 – Allocation of Resources (Low)

Control

The organization:
a. Includes a determination of information security requirements for the information system in mission/business process planning;

b. Determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process;
c. Includes information security requirements in mission/business case planning, and
d. Establishes a discrete line item in CMS' programming and budgeting documentation for the implementation and management of information systems security.

Applicability: All	**Reference(s):** FISCAM: CM-3, IN-2, SD-1, SM-1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SA-2.1

Assessment Objective

Determine if:
the organization includes a determination of the information security requirements for the information system in mission/business process planning;

the organization determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process;

the organization establishes a discrete line item for information security in organizational programming and budgeting documentation;

the organization establishes a discrete line item in CMS' programming and budgeting documentation for the implementation and management of information systems security.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing the allocation of resources to information security requirements; organizational programming and budgeting documentation; other relevant documents or records.

SA-3 – Life Cycle Support (Low)

Control

The organization:
a. Manages the information system using the information security steps of IEEE 12207.0 standard for SDLC, as provided in the CMS Integrated IT Investment & System Life Cycle Framework (ILC);
b. Defines and documents information system security roles and responsibilities throughout the system development life cycle; and
c. Identifies individuals having information system security roles and responsibilities.

Applicability: All	**Reference(s):** FISCAM: AC-2, AS-3, AS-5, BP-1, BP-2, BP-3, BP-4, CM-1, CM-3, CP-3, DA-1, IN-1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SA-3.1

Assessment Objective

Determine if:
the organization manages the information system using the information security steps of IEEE 12207.0 standard for SDLC, as provided in the CMS Integrated IT Investment & System Life Cycle Framework (ILC);

the organization defines and documents information system security roles and responsibilities throughout the system development life cycle;

the organization identifies individuals having information system security roles and responsibilities.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing the integration of information security into the system development life cycle process; information system development life cycle documentation; other relevant documents or records.

SA-4 – Acquisitions (Low)

Control

The organization includes the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards:
a. Security functional requirements/specifications;
b. Security-related documentation requirements; and

c. Developmental and evaluation-related assurance requirements.

Implementation Standard(s)

1. Each contract and Statement of Work (SOW) that requires development or access to CMS information must include language requiring adherence to CMS security policies and standards, define security roles and responsibilities, and receive approval from CMS officials.

Guidance

The acquisition documents for CMS information systems, CMS information system components, and CMS information system services include, either explicitly or by reference, security requirements that describe: (i) required security capabilities (i.e., security needs and, as necessary, specific security controls and other specific FISMA requirements); (ii) required design and development processes; (iii) required test and evaluation procedures; and (iv) required documentation.
Solicitation Documents:
Solicitation documents (e.g., Request for Proposal) for any CMS information system shall include, either explicitly or by reference, security requirements that describe the required:
- Security capabilities;
- Design and development processes;
- Test and evaluation procedures; and
- Documentation.
The requirements in the solicitation documents shall permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented.
Use of Evaluated and Validated Products:
For acquisition of security and security-enabled commercial-off-the-shelf (COTS) information technology products, when multiple products meet CMS requirements, preference shall be given to products that have been evaluated and validated through one or more of the following sources:
1. The National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme;
2. The International Common Criteria Recognition Arrangements; and
3. The NIST Cryptographic Module Validation Program.

Applicability: All	**Reference(s):** FISCAM: AS-1, CM-3, SM-7	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SA-4.1

Assessment Objective

Determine if:
the organization includes the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards:
- security functional requirements/specifications;
- security-related documentation requirements;
- developmental and evaluation-related assurance requirements.

the organization meets all the requirements specified in the applicable implementation standard(s).

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; acquisition contracts for information systems or services; other relevant documents or records.

SA-5 – Information System Documentation (Low)

Control

The organization:
a. Obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes:
- Secure configuration, installation, and operation of the information system;
- Effective use and maintenance of security features/functions; and
- Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; and
b. Obtains, protects as required, and makes available to authorized personnel, user documentation for the information system that describes:

- User-accessible security features/functions and how to effectively use those security features/functions;
- Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and
- User responsibilities in maintaining the security of the information and information system; and
c. Documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.

Implementation Standard(s)

1. Develop system documentation to describe the system and to specify the purpose, technical operation, access, maintenance, and required training for administrators and users.
2. Maintain an updated list of related system operations and security documentation.
3. Update documentation upon changes in system functions and processes. Must include date and version number on all formal system documentation.

Guidance

The inability of the organization to obtain necessary information system documentation may occur, for example, due to the age of the system and/or lack of support from the vendor/contractor. In those situations, organizations may need to recreate selected information system documentation if such documentation is essential to the effective implementation and/or operation of security controls.

Applicability: All	**Reference(s):** FISCAM: AS-1, AS-2, AS-3, AS-4, AS-5, BP-1, BP-2, BP-3, BP-4, CM-2, CM-3, CP-2, DA-1, IN-1, IN-2, SD-1, SD-2; IRS-1075: 5.6.1.3#1.3	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SA-5.1

Assessment Objective

Determine if:
the organization obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes:
- secure configuration, installation, and operation of the information system;
- effective use and maintenance of the security features/functions;
- known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;

the organization obtains, protects as required, and makes available to authorized personnel, user documentation for the information system that describes:
- user-accessible security features/functions and how to effectively use those security features/functions;
- methods for user interaction with the information system, which enables individuals to use the system in a more secure manner;
- user responsibilities in maintaining the security of the information and information system;

the organization documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.

the organization meets all the requirements specified in the applicable implementation standard(s).

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing information system documentation; information system documentation including administrator and user guides; records documenting attempts to obtain unavailable or nonexistent information system documentation; other relevant documents or records.

ASSESSMENT PROCEDURE: SA-5.FIS-1

Assessment Objective

Determine if:
the organization develops information system documentation for operating the system that includes:
- operational instructions and
- appropriate end user control, balancing, and verification features and procedures.

the organization disseminates information system documentation to appropriate elements within the organization;

responsible parties within the organization periodically review information system documentation;

the organization updates information system documentation when organizational review indicates updates are required or changes are made to the system.

Assessment Methods And Objects

Examine: Information system documentation; other relevant documents or records.

SA-6 – Software Usage Restrictions (Low)

Control

The organization:
a. Uses software and associated documentation in accordance with contract agreements and copyright laws;
b. Employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution; and
c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Guidance

Tracking systems can include, for example, simple spreadsheets or fully automated, specialized applications depending on the needs of the organization.

Applicability: All	**Reference(s):** FISCAM: CM-3, CM-5; IRS-1075: 4.7.3#1.2	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SA-6.1

Assessment Objective

Determine if:
the organization uses software and associated documentation in accordance with contract agreements and copyright laws;

the organization employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution;

the organization controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing software usage restrictions; site license documentation; list of software usage restrictions; other relevant documents or records.

SA-7 – User-Installed Software (Low)

Control

The organization prohibits users from downloading or installing software, unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, explicit rules govern the installation of software by users.

Implementation Standard(s)

1. If user installed software is authorized, ensure that business rules and technical controls enforce the documented authorizations and prohibitions.

Guidance

If provided the necessary privileges, users have the ability to install software. The organization identifies what types of software installations are permitted (e.g., updates and security patches to existing software) and what types of installations are prohibited (e.g., software whose pedigree with regard to being potentially malicious is unknown or suspect).

Applicability: All	**Reference(s):** FISCAM: CM-3, CM-5	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SA-7.1

Assessment Objective

Determine if:
the organization identifies and documents (as appropriate) explicit rules to be enforced when governing the installation of software by users;

the organization (or information system) enforces explicit rules governing the installation of software by users.

the organization meets all the requirements specified in the applicable implementation standard(s).

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing user installed software; list of rules governing user installed software; network traffic on the information system; other relevant documents or records.

SA-9 – External Information System Services (Low)

Control

The organization prohibits service providers from outsourcing any system function outside the U.S. or its territories, unless explicitly authorized, in writing, by the CMS CIO or his/her designated representative with concurrence from CMS' personnel security department. If service providers are authorized to outsource outside the U.S. or its territories, the organization:
a. Requires that providers of external information system services comply with CMS information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
b. Defines and documents oversight and user roles and responsibilities with regard to external information system services;
c. Ensures that service level agreements define expectations of performance, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance; and
d. Monitors CMS security control compliance by external service providers.

Guidance

An external information system service is a service that is implemented outside of the authorization boundary of the CMS information system (i.e., a service that is used by, but not a part of, the CMS information system). Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain exchanges. The responsibility for adequately mitigating risks arising from the use of external information system services remains with the authorizing official. Authorizing officials require that an appropriate chain of trust be established with external service providers when dealing with the many issues associated with information security. For services external to the organization, a chain of trust requires that the organization establish and retain a level of confidence that each participating provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered to the organization. The extent and nature of this chain of trust varies based on the relationship between the organization and the external provider. Where a sufficient level of trust cannot be established in the external services and/or service providers, the organization employs compensating security controls. The external information system services documentation includes government, service provider, and end user security roles and responsibilities, and any service-level agreements. Service-level agreements define the expectations of performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instance of noncompliance.

Applicability: All	**Reference(s):** FISCAM: AS-1, SM-7; HIPAA: 164.314(b)(2)(iii); HSPD 7: D(8); IRS-1075: 5.6.1.3#1.4	**Related Controls Requirement(s):** CA-3

ASSESSMENT PROCEDURE: SA-9.1

Assessment Objective

Determine if:
the organization prohibits service providers from outsourcing any system function outside the U.S. or its territories, unless explicitly authorized, in writing, by the CMS CIO with concurrence from CMS' personnel security department;

if authorized, the organization requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

if authorized, the organization defines and documents government oversight, and user roles and responsibilities with regard to external information system services;

if authorized, the organization ensures that service level agreements define expectations of performance, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance;

if authorized, the organization monitors security control compliance by external service providers.

Assessment Methods And Objects

Examine: System and services acquisition policy; procedures addressing external information system services; acquisition contracts and service level agreements; organizational security requirements and security specifications for external provider services; security control assessment evidence from external providers of information system services; other relevant documents or records.

System and Communications Protection (SC) – *Technical*

SC-1 – System and Communications Protection Policy and Procedures (Low)

Control

The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:
a. A formal, documented system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.

Guidance

This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the system and communications protection family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The system and communications protection policy can be included as part of the general information security policy for the organization. System and communications protection procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system and communications protection policy.

Applicability: All	**Reference(s):** FISCAM: AS-1, CM-5, SM-1, SM-3; IRS-1075: 5.6.3.4#1, 5.6.3.4#2	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SC-1.1

Assessment Objective

Determine if:
the organization develops and formally documents system and communications protection policy;

the organization system and communications protection policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented system and communications protection policy to elements within the organization having associated system and communications protection roles and responsibilities;

the organization develops and formally documents system and communications protection procedures;

the organization system and communications protection procedures facilitate implementation of the system and communications protection policy and associated system and communications protection controls;

the organization disseminates formal documented system and communications protection procedures to elements within the organization having associated system and communications protection roles and responsibilities;

the organization reviews/updates the system and communications protection policy and procedures within every three hundred sixty-five (365) days.

Assessment Methods And Objects

Examine: System and communications protection policy and procedures; other relevant documents or records.

SC-5 – Denial of Service Protection (Low)

Control

The information system protects against or limits the effects of the following types of denial of service attacks defined on the following sites or in the following documents:

- SANS Organization www.sans.org/dosstep;
- SANS Organization's Roadmap to Defeating DDoS www.sans.org/dosstep/roadmap.php; and
- NIST CVE List http://checklists.nist.gov/home.cfm.

Guidance

A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect devices on an organization's internal network from being directly affected by denial of service attacks. Employing increased capacity and bandwidth combined with service redundancy may reduce the susceptibility to some denial of service attacks.

Applicability: All	**Reference(s):** FISCAM: AC-5	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SC-5.1

Assessment Objective

Determine if:
the organization defines in the security plan, explicitly or by reference, the types of denial of service attacks (or provides references to sources of current denial of service attacks) that can be addressed by the information system;

the information system protects against or limits the effects of the organization-defined or referenced types of denial of service attacks.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing denial of service protection; information system design documentation; security plan; information system configuration settings and associated documentation; other relevant documents or records.

SC-7 – Boundary Protection (Low)

Control

The information system:
a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and
b. Connects to external networks or information systems only through managed interfaces consisting of automated boundary protection devices arranged in accordance with an organizational security architecture.

Implementation Standard(s)

1. Ensure that access to all proxies is denied, except for those hosts, ports, and services that are explicitly required.
2. Although not required, it is recommended that stateful inspection hardware and software is utilized.

Guidance

Restricting external web traffic only to organizational web servers within managed interfaces and prohibiting external traffic that appears to be spoofing an internal address as the source are examples of restricting and prohibiting communications. Managed interfaces employing boundary protection devices include, for example, proxies, gateways, routers, firewalls, guards, or encrypted tunnels arranged in an effective security architecture (e.g., routers protecting firewalls and application gateways residing on a protected subnetwork commonly referred to as a demilitarized zone or DMZ).
The organization considers the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may include third-party provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions. When this situation occurs, the organization implements appropriate compensating security controls.

Applicability: All	**Reference(s):** FISCAM: AC-1, AS-2	**Related Controls Requirement(s):** AC-4, CA-3, MP-4, RA-2

ASSESSMENT PROCEDURE: SC-7.1

Assessment Objective

Determine if:

the organization defines the external boundary of the information system;

the organization defines key internal boundaries of the information system;

the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system;

the information system connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

the organization meets all the requirements specified in the applicable implementation standard(s).

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the information system; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; enterprise security architecture documentation; other relevant documents or records.

SC-12 – Cryptographic Key Establishment and Management (Low)

Control

When cryptography is required and used within the information system, the organization establishes and manages cryptographic keys for required cryptography employed within the information system.

Guidance

Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. In addition to being required for the effective operation of a cryptographic mechanism, effective cryptographic key management provides protections to maintain the availability of the information in the event of the loss of cryptographic keys by users.

Applicability: All	**Reference(s):** FISCAM: AC-4; IRS-1075: 5.7.1#1	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SC-12.1

Assessment Objective

Determine if the organization establishes and manages cryptographic keys for required cryptography employed within the information system.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing cryptographic key management and establishment; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

SC-13 – Use of Cryptography (Low)

Control

When cryptographic mechanisms are used, the information system implements required cryptographic protections using cryptographic modules that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Applicability: All	**Reference(s):** FISCAM: AC-4; HIPAA: 164.312(a)(2)(iv), 164.312(e)(2)(ii); IRS-1075: 4.7.2#1, 5.6.3.4#2, 5.6.3.4#4.2-3	**Related Controls Requirement(s):** AC-3, SC-8.Std.1, SC-9(1)

ASSESSMENT PROCEDURE: SC-13.1

Assessment Objective

Determine if when cryptographic mechanisms are used, the information system implements cryptographic protections using cryptographic modules that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing use of cryptography; information system design documentation; information system configuration settings and associated documentation; cryptographic module validation certificates; other relevant documents or records.

SC-13(1) – Enhancement (Low)		
Control When cryptographic mechanisms are used, the organization employs, at a minimum, FIPS 140-2 compliant and NIST-validated cryptography to protect unclassified information.		
Applicability: All	**Reference(s):**	**Related Controls Requirement(s):**
ASSESSMENT PROCEDURE: SC-13(1).1		
Assessment Objective Determine if when cryptographic mechanisms are used, the organization employs, at a minimum, FIPS-validated cryptography to protect unclassified information. **Assessment Methods And Objects** **Examine:** System and communications protection policy; procedures addressing use of cryptography; FIPS cryptography standards; information system design documentation; information system configuration settings and associated documentation; cryptographic module validation certificates; other relevant documents or records.		
SC-14 – Public Access Protections (Low)		
Control The information system protects the integrity and availability of publicly available information and applications. **Implementation Standard(s)** 1. Ensure that network access controls, operating system file permissions, and application configurations protect the integrity of information stored, processed, and transmitted by publicly accessible systems, as well as the integrity of publicly accessible applications. 2. If e-authentication is required and implemented in conjunction with or related to public access protections, refer to ARS Appendix D: E-authentication Standard.		
Guidance The purpose of this control is to ensure that organizations explicitly address the protection needs for public information and applications with such protection likely being implemented as part of other security controls. CMS refers to the National Institute of Standards and Technology (NIST) SP 800-63 for technical controls. The ARS Appendix D: E-authentication Standard provides a summary for remote access controls.		
Applicability: All	**Reference(s):** FISCAM: AC-2, AC-3	**Related Controls Requirement(s):**
ASSESSMENT PROCEDURE: SC-14.1		
Assessment Objective Determine if: the information system protects the integrity and availability of publicly available information and applications. the organization meets all the requirements specified in the applicable implementation standard(s). **Assessment Methods And Objects** **Examine:** System and communications protection policy; procedures addressing public access protections; access control policy and procedures; boundary protection procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.		
SC-15 – Collaborative Computing Devices (Low)		
Control The organization prohibits running collaborative computing mechanisms, unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the authorization shall specifically identify allowed mechanisms, allowed purpose, and the information system upon which the mechanisms can be used. The information system: a. Prohibits remote activation of collaborative computing devices; and b. Provides an explicit indication of use to users physically present at the devices.		

Guidance

Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated.

Applicability: All	**Reference(s):** FISCAM: AC-3	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SC-15.1

Assessment Objective

Determine if:
the organization prohibits running collaborative computing mechanisms, unless explicitly authorized, in writing, by the CIO or his/her designated representative;

if authorized, the authorization shall specifically identify allowed mechanisms, allowed purpose, and the information system upon which the mechanisms can be used;

if authorized, the information system prohibits remote activation of collaborative computing devices;

if authorized, the information system provides an explicit indication of use to users physically present at the devices.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing collaborative computing; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

SC-20 – Secure Name /Address Resolution Service (Authoritative Source) (Low)

Control

The information system provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries.

Guidance

This control enables remote clients to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. A domain name system (DNS) server is an example of an information system that provides name/address resolution service. Digital signatures and cryptographic keys are examples of additional artifacts. DNS resource records are examples of authoritative data. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to assure the authenticity and integrity of response data. The DNS security controls are consistent with, and referenced from, OMB Memorandum 08-23.

Applicability: All	**Reference(s):** FISCAM: AC-2	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SC-20.1

Assessment Objective

Determine if the information system provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing secure name/address resolution service (authoritative source); information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

SC-20(1) – Enhancement (Low)

Control

The information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.

Guidance

An example means to indicate the security status of child subspaces is through the use of delegation signer (DS) resource records in the DNS.

Applicability: All	**Reference(s):**	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SC-20(1).1

Assessment Objective

Determine if:
the information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces;

the information system, when operating as part of a distributed, hierarchical namespace, enable verification of a chain of trust among parent and child domains (if the child supports secure resolution services).

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing secure name/address resolution service (authoritative source); information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

SC-CMS-2 – Website Usage (Low)

Control

CMS web sites are operated within the restrictions addressed in OMB directives M-10-22 "Guidance for Online Use of Web Measurement and Customization Technologies" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications" and applicable CMS and DHHS directives and instruction.

Guidance

Monitor the CMS and DHHS security programs to determine is there are any modified directives and instruction.

Applicability: All	**Reference(s):**	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SC-CMS-2.1

Assessment Objective

Determine if the organization maintains CMS websites within restrictions addressed in OMB directives M-10-22 "Guidance for Online Use of Web Measurement and Customization Technologies" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications" and applicable CMS and DHHS directives and instruction.

Assessment Methods And Objects

Examine: CMS web site baseline and change management documentation for appropriate configurations.

System and Information Integrity (SI) – *Operational*

SI-1 – System and Information Integrity Policy and Procedures (Low)

Control

The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days:
a. A formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.

Guidance

This control is intended to produce the policy and procedures that are required for the effective implementation of CMS security controls and control enhancements in the system and information integrity family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The system and information integrity policy can be included as part of the general information security policy for the organization. System and information integrity procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system and information integrity policy.

Applicability: All	**Reference(s):** FISCAM: AS-1, BP-1, BP-2, BP-3, BP-4, CP-2, SM-1, SM-3; HIPAA: 164.312(c)(1); IRS-1075: 5.6.2.5#1.1-2	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SI-1.1

Assessment Objective

Determine if:
the organization develops and formally documents system and information integrity policy;

the organization system and information integrity policy addresses:
- purpose;
- scope;
- roles and responsibilities;
- management commitment;
- coordination among organizational entities;
- compliance;

the organization disseminates formal documented system and information integrity policy to elements within the organization having associated system and information integrity roles and responsibilities;

the organization develops and formally documents system and information integrity procedures;

the organization system and information integrity procedures facilitate implementation of the system and information integrity policy and associated system and information integrity controls;

the organization disseminates formal documented system and information integrity procedures to elements within the organization having associated system and information integrity roles and responsibilities.

the organization reviews/updates the system and information integrity policy and procedures within every three hundred sixty-five (365) days.

Assessment Methods And Objects

Examine: System and information integrity policy and procedures; other relevant documents or records.

SI-2 – Flaw Remediation (Low)

Control

The organization:

a. Identifies, reports, and corrects information system flaws;
b. Tests software updates related to flaw remediation for effectiveness and potential side effects on CMS information systems before installation; and
c. Incorporates flaw remediation into the organizational configuration management process.

Implementation Standard(s)

1. Correct identified information system flaws on production equipment in a timeframe based on the National Vulnerability Database (NVD) Vulnerability Severity Rating of the flaw: flaws rated as High severity within seven (7) calendar days; Medium severity within fifteen (15) calendar days; and all others within thirty (30) calendar days.
(a) Evaluate system security patches, service packs, and hot fixes in a test bed environment to determine the effectiveness and potential side effects of such changes, and
(b) Manage the flaw remediation process centrally.

Guidance

The organization identifies CMS information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws) and reports this information to designated organizational officials with information security responsibilities (e.g., senior information security officers, information system security managers, information systems security officers). The organization (including any contractor to the organization) installs security-relevant software updates (e.g., patches, service packs, and hot fixes) within the CMS-designated time period. Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling, are also addressed expeditiously. Organizations are encouraged to use resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in CMS information systems. By requiring that flaw remediation be incorporated into the organizational configuration management process, it is the intent of this control that required/anticipated remediation actions are tracked and verified. An example of expected flaw remediation that would be so verified is whether the procedures contained in US-CERT guidance and Information Assurance Vulnerability Alerts have been accomplished.

Applicability: All	**Reference(s):** FISCAM: AS-3, CM-5; HIPAA: 164.308(a)(1)(i); IRS-1075: 5.6.2.5#1.1-2	**Related Controls Requirement(s):** CA-2, CA-4, CA-7, CM-3, IR-4, SI-11

ASSESSMENT PROCEDURE: SI-2.1

Assessment Objective

Determine if:
the organization identifies, reports, and corrects information system flaws;

the organization tests software updates related to flaw remediation for effectiveness before installation;

the organization tests software updates related to flaw remediation for potential side effects on organizational information systems before installation;

the organization incorporates flaw remediation into the organizational configuration management process.

the organization meets all the requirements specified in the applicable implementation standard(s).

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing flaw remediation; list of flaws and vulnerabilities potentially affecting the information system; list of recent security flaw remediation actions performed on the information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct information system flaws); test results from the installation of software to correct information system flaws; other relevant documents or records.

SI-2(1) – Enhancement (Low)

Control

The organization centrally manages the flaw remediation process and installs software updates automatically.

Guidance

Due to information system integrity and availability concerns, organizations give careful consideration to the methodology used to carry out automatic updates.

Applicability: All	**Reference(s):**	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SI-2(1).1

Assessment Objective

Determine if:
the organization centrally manages the flaw remediation process;

the organization installs software updates automatically.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing flaw remediation; automated mechanisms supporting centralized management of flaw remediation and automatic software updates; information system design documentation; information system configuration settings and associated documentation; list of information system flaws; list of recent security flaw remediation actions performed on the information system; other relevant documents or records.

SI-2(2) – Enhancement (Low)

Control

The organization employs automated mechanisms monthly to determine the state of information system components with regard to flaw remediation.

Applicability: All	**Reference(s):**	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SI-2(2).1

Assessment Objective

Determine if:
the organization defines the frequency of employing automated mechanisms to determine the state of information system components with regard to flaw remediation;

the organization employs automated mechanisms in accordance with the organization-defined frequency to determine the state of information system components with regard to flaw remediation.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing flaw remediation; automated mechanisms supporting flaw remediation; information system design documentation; information system configuration settings and associated documentation; list of information system flaws; list of recent security flaw remediation actions performed on the information system; information system audit records; other relevant documents or records.

SI-3 – Malicious Code Protection (Low)

Control

The organization:
a. Employs malicious code protection mechanisms at CMS information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code:
- Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or
- Inserted through the exploitation of information system vulnerabilities;
b. Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with CMS configuration management policy and procedures;
c. Configures malicious code protection mechanisms to:
- Perform critical system file scans during system boot, information system scans using the frequency specified in Implementation Standard 1, and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and
- Block and quarantine malicious code and send alert to administrator in response to malicious code detection; and
d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

Implementation Standard(s)

1. Desktop malicious code scanning software is configured to perform critical system file scans once a week.

Guidance

Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, and remote-access servers. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode) or contained within a compressed file. Removable media includes, for example, USB devices, diskettes, or compact disks. A variety of technologies and methods exist to limit or eliminate the effects of malicious code attacks. Pervasive configuration management and strong software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect CMS missions and business functions. Traditional malicious code protection mechanisms are not built to detect such code. In these situations, organizations must rely instead on other risk mitigation measures to include, for example, secure coding practices, trusted procurement processes, configuration management and control, and monitoring practices to help ensure that software does not perform functions other than those intended.

Applicability: All	**Reference(s):** FISCAM: CM-5; IRS-1075: 5.6.2.5#1.3	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SI-3.1

Assessment Objective

Determine if:
the organization employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code:
- transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or
- inserted through the exploitation of information system vulnerabilities;

the organization employs malicious code protection mechanisms at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code:
- transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or
- inserted through the exploitation of information system vulnerabilities;

the organization updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with configuration management policy and procedures defined in CM-1;

the organization defines one or more of the following actions to be taken in response to malicious code detection:
- block malicious code;
- quarantine malicious code; and/or
- send alert to administrator;

the organization configures malicious code protection mechanisms to:
- perform periodic scans of the information system in accordance with organization-defined frequency;
- perform real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy;
- take organization-defined action(s) in response to malicious code detection;

the organization addresses the receipt of false positives during malicious code:
- detection and eradication;
- the resulting potential impact on the availability of the information system.

the organization meets all the requirements specified in the applicable implementation standard(s).

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing malicious code protection; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records.

SI-3(1) – Enhancement (Low)

Control

The organization centrally manages malicious code protection mechanisms.

Applicability: All	**Reference(s):**	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SI-3(1).1

Assessment Objective

Determine if the organization centrally manages malicious code protection mechanisms.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing malicious code protection; information system design documentation; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records.

SI-3(2) – Enhancement (Low)

Control

The information system automatically updates malicious code protection mechanisms (including signature definitions).

Applicability: All	**Reference(s):**	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SI-3(2).1

Assessment Objective

Determine if the information system automatically updates malicious code protection mechanisms, including signature definitions.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing malicious code protection; information system design documentation; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records.

SI-4 – Information System Monitoring (Low)

Control

The organization:
a. Monitors events on the information system in accordance with CMS Information Security Incident Handling and Breach Analysis/Notification Procedure and detects information system attacks;
b. Identifies unauthorized use of the information system;
c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization;
d. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to CMS operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; and
e. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.

Implementation Standard(s)

1. Install IDS devices at network perimeter points and host-based IDS sensors on critical servers.

Guidance

Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the system (e.g., within internal organizational networks and system components). Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include, for example, at selected perimeter locations and near server farms supporting critical applications, with such devices typically being employed at the managed interfaces associated with controls SC-7 and AC-17. The Einstein network monitoring device from the Department of Homeland Security is an example of a system monitoring device. The granularity of the information collected is determined by the organization based on its monitoring objectives and the capability of the information system to support such activities. An example of a specific type of transaction of interest to the organization with regard to monitoring is Hyper Text Transfer Protocol (HTTP) traffic that bypasses organizational HTTP proxies, when use of such proxies is required.

Applicability: All	**Reference(s):** FISCAM: AC-5, DA-1, SM-5; HIPAA: 164.308(a)(5)(ii)(B); IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#1.4	**Related Controls Requirement(s):** AC-8, AU-4, CM-6

ASSESSMENT PROCEDURE: SI-4.1

Assessment Objective

Determine if:
the organization monitors events on the information system in accordance with CMS Information Security Incident Handling and Breach Analysis/Notification Procedure and detects information system attacks;

the organization identifies unauthorized use of the information system;

the organization deploys monitoring devices:
- strategically within the information system to collect organization-determined essential information;
- at ad hoc locations within the system to track specific types of transactions of interest to the organization;

the organization heightens the level of information system monitoring activity whenever there is an indication of increased risk to CMS operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;

the organization obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.

the organization meets all the requirements specified in the applicable implementation standard(s).

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; other relevant documents or records.

SI-4(1) – Enhancement (Low)

Control

The organization interconnects and configures individual intrusion detection tools into a systemwide intrusion detection system using common protocols.

Applicability: All	**Reference(s):**	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SI-4(1).1

Assessment Objective

Determine if the organization interconnects and configures individual intrusion detection tools into a system-wide intrusion detection system using common protocols.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols; other relevant documents or records.

SI-4(5) – Enhancement (Low)

Control

The information system provides near real-time alerts when the following indications of compromise or potential compromise occur:
(a) Presence of malicious code,
(b) Unauthorized export of information,
(c) Signaling to an external information system, or
(d) Potential intrusions.

Guidance

Alerts may be generated, depending on the organization-defined list of indicators, from a variety of sources, for example, audit records or input from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers.

Applicability: All	**Reference(s):**	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SI-4(5).1

Assessment Objective

Determine if:
the organization defines indicators of compromise or potential compromise to the security of the information system;

the information system provides near real-time alerts when any of the organization-defined list of compromise or potential compromise indicators occurs.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; security plan; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; other relevant documents or records.

SI-5 – Security Alerts, Advisories, and Directives (Low)

Control

The organization:
a. Receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis;
b. Generates internal security alerts, advisories, and directives as deemed necessary;
c. Disseminates security alerts, advisories, and directives to appropriate personnel; and
d. Implements security directives in accordance with established time frames, or notifies CMS of the degree of noncompliance.

Guidance

Security alerts and advisories are generated by the United States Computer Emergency Readiness Team (US-CERT) to maintain situational awareness across the federal government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives. Compliance to security directives is essential due to the critical nature of many of these directives and the potential immediate adverse affects on CMS operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner.

Applicability: All	**Reference(s):** FISCAM: AC-5, AS-3, CM-5, DA-1, SM-5	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: SI-5.1

Assessment Objective

Determine if:
the organization receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis;

the organization generates internal security alerts, advisories, and directives;

the organization defines personnel (identified by name and/or by role) who should receive security alerts, advisories, and directives;

the organization disseminates security alerts, advisories, and directives to organization-identified personnel;

the organization implements security directives in accordance with established time frames, or notifies CMS of the degree of noncompliance.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing security alerts and advisories; records of security alerts and advisories; other relevant documents or records.

SI-8 – Spam Protection (Low)

Control

The organization:
a. Employs spam protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means; and
b. Updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with CMS configuration management policy and procedures.

Guidance

Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, and remote-access servers.

Applicability: All	Reference(s): FISCAM: CM-5; HIPAA: 164.308(a)(1)(i)	Related Controls Requirement(s):

ASSESSMENT PROCEDURE: SI-8.1

Assessment Objective

Determine if:
the organization employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means;

the organization employs spam protection mechanisms at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means;

the organization updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures defined in CM-1.

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing spam protection; information system design documentation; spam protection mechanisms; information system configuration settings and associated documentation; other relevant documents or records.

SI-12 – Information Output Handling and Retention (Low)

Control

The organization handles and retains both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

Implementation Standard(s)

1. Retain output, including, but not limited to audit records, system reports, business and financial reports, and business records, from the information system in accordance with CMS Policy and all applicable National Archives and Records Administration (NARA) requirements.

Guidance

The output handling and retention requirements cover the full life cycle of the information, in some cases extending beyond the disposal of the information system. The National Archives and Records Administration provides guidance on records retention.

Applicability: All	Reference(s): FISCAM: BP-2, BP-3; IRS-1075: 5.6.2.5#1.1-2, 5.6.2.5#2.2	Related Controls Requirement(s):

ASSESSMENT PROCEDURE: SI-12.1

Assessment Objective

Determine if:
the organization handles both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements;

the organization retains both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

the organization meets all the requirements specified in the applicable implementation standard(s).

Assessment Methods And Objects

Examine: System and information integrity policy; procedures addressing information system output handling and retention; media protection policy and procedures; information retention records, other relevant documents or records.